Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Creación de una guía para el control del cumplimiento de los derechos que el Reglamento de Protección de Datos Europeo ofrece a los consumidores.

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: [Adrián Castellano Navarro]

Tutor: [Juan Vicente Oltra Gutiérrez]

[2017-2018]

Resumen

El día veinticinco de mayo de dos mil dieciocho entró en vigor el nuevo reglamento de protección de datos. Este reglamento presenta un conjunto de derechos y obligaciones a sus consumidores, para así estar conforme al reglamento de datos europeo, dado que todos los países de la unión europea han de adaptarse a dicho reglamento.

Como las empresas necesitan adaptarse al nuevo reglamento para de esta forma evitar las sanciones de hasta veinte millones de euros, se ha desarrollado una guía para que las empresas puedan adaptarse al nuevo reglamento, además de que como trabajo adicional se ha desarrollado una página web mediante la herramienta Drupal, en la cual tras contestar a un cuestionario nos devolverá un listado con los puntos que no están conforme al reglamento para así facilitar el conocimiento y corrección de dichos puntos.

Palabras clave: Protección de datos, página web, Drupal, guía, informe.

Abstract

The date of may, twuenty-five of twuenty eighteen the new protection data regulation become effective. This new regulation introduce a set of rights and obligations to the consumers of this regulation, with the objective of being in order with the european protection data regulation, because all the countries in the european union must adapt to the aforesaid regulation.

Companies need to adapt to the new regulation, for in this way prevent the sanctions that can rise to twenty million euros, a guide has been developed with the objetive of helping companies to adapt to the new regulation, Furthermore as a aditional work a web site has been developed by using Drupal, in this web site you have the option of answering a questionnaire which returns a list of the areas that are not in order with the regulation, with the objective of make easier the knowledge and correction of this areas.

Keywords: Data protection, Web Site, Drupal, Guide, Report.

Tabla de contenidos

1. Introducción

El día veinticinco de mayo de dos mil dieciocho entró en vigor el nuevo reglamento de protección de datos en España, este nuevo reglamento surge para que España se adapte al reglamento de protección de datos europeo. Todos los países de la unión europea tienen el deber de adaptarse a las normas de este reglamento de protección de datos europeo.

Este nuevo reglamento supone un cambio en el marco jurídico al que las empresas deberán adaptarse, ya que esta nueva ley, introduce un conjunto de derechos y obligaciones novedosos en España, en referente al tratamiento de los datos personales.

Para el desarrollo de la guía se ha realizado un estudio del anteproyecto de ley de protección de datos hecho público por la Agencia española de protección de datos y por el reglamento de protección de datos europeo dos mil dieciséis, barra, seiscientos setenta y nueve del parlamento europeo y del consejo con feche de veintisiete de abril de dos mil dieciséis.

También se ha analizado el reglamento e-privacy el cual forma parte del reglamento de datos europeo, pero es una norma la cual puede afectar a una empresa, especialmente si esta se dedica al ámbito publicitario.

Como metodología utilizada para el desarrollo de esta guía se ha realizado un seguimiento de los datos en lo que sería un tratamiento de datos corriente. Para cada área, se relata cuáles son las obligaciones que debe cumplir una empresa y en que artículos se refleja y qué es lo que dictan dichos artículos.

Para el uso de esta guía es importante que el usuario diferencie entre los diferentes tipos de empresa, es decir, pública privada o mixta, ya que hay apartados en los que se producen ciertas excepciones al tratarse de empresas del sector público.

Adicionalmente, se ha realizado una página web en la que se permite a los usuarios realizar un cuestionario donde se realizan las preguntas que se formulan en cada área. Dicho cuestionario devuelve un listado con todos aquellos puntos que la empresa no cumple o podría mejorar.

2. Objetivos

El principal objetivo es la realización de una guía con la que se pueda comprobar el control del cumplimiento de los derechos que el reglamento de datos europeo ofrece a sus consumidores.

También como objetivo está presente el poder ofrecer una guía para que las empresas puedan adaptarse al nuevo reglamento.

Ofrecer una página web con la herramienta del cuestionario con tal de ofrecer una herramienta más accesible la cual puede ser utilizada para realizar una auditoría por una persona dentro de la empresa o una persona encargada a realizar la auditoría con conocimientos de la empresa, la cual, ofrezca un listado con aquellas áreas a mejorar.

Aplicar los conocimientos de la asignatura Diseño de sitios web impartida en la universidad politécnica de Valencia.

Ampliar mis conocimientos y aprender sobre el reglamento y así conocer también mis derechos y poder aplicar correctamente estos conocimientos cuando en mi futuro profesional se da la situación de que debo realizar un tratamiento de datos personales.

3. Análisis

¿Cómo afecta la norma a un profesional informático?

Cuando los datos personales se tratan de manera informatizada, la empresa debe tener una metodología acorde para no quebrantar la legislación en materia de protección de datos y dejando los datos personales de una gran cantidad de personas vulnerables a los intereses de tanto las empresas que recogen los datos, como de las empresas de terceros interesadas en dichos datos.

Unos datos mal tratados pueden perjudicar a la vida de una persona además de que no hay que perder la noción de que los datos pertenecen a personas reales y un mal tratamiento puede perjudicar a una persona.

Esta norma afecta a los profesionales informáticos de una manera directa, ya que, como se estudia a lo largo del grado de ingeniería informática, la ley de protección de datos es una de las leyes que más afectan a un profesional informático en su vida laboral.

Como se detalla en esta guía, un miembro de la empresa debe tratar los datos de los afectados tal y como se estipula a lo largo de la ley, siendo necesarios guardar registros de los accesos a los datos, modificaciones de los mismos, siendo clave que estas acciones sean realizadas bajo el uso de material informático.

También la norma detalla las medidas de seguridad necesarias, así como la portabilidad de los ficheros los cuales contienen datos personales, siendo tan importante que el quebrantar la norma puede llevar a la empresa que incumpla la norma a multas de hasta unos veinte millones de euros.

Áreas que evaluar en una auditoría

Para el desarrollo de la organización de esta guía se ha planteado un seguimiento de los datos desde el momento en el que se guardan del cliente, hasta que finalmente son destruidos.

- Comprobar si se informa al cliente que sus datos se usarán para un objetivo en un documento correspondiente y que siga la normativa del reglamento. En este apartado entraría todo lo relacionado al caso que sea para cuando se recojan los datos del cliente, es decir, personas adultas, videovigilancia, si se recoge a menores, a persona con algún tipo de discapacidad especial.

- A continuación, pasaríamos a comprobar en cada empresa el papel del responsable y también del o de los encargados del tratamiento y de si siguen el reglamento europeo.

- Después Analizaríamos como se tratan los datos para todos los tipos de datos que diferenciamos en el índice.

- A continuación, realizaríamos una comprobación del lugar de almacenamiento de los datos y de si estos cumplen la normativa de seguridad que estipula la norma europea.

- Después analizaríamos si han seguido algún código de conducta y de si han inscrito los ficheros en la Agencia española de protección de datos.

- A continuación, analizaríamos si dicha empresa contempla los derechos de los afectados para acceder, modificar, actualizar o solicitar la eliminación de los datos.

- Analizar, en el caso de que se transfieran los datos a otros países, si estos pertenecen a la unión europea, o al conjunto de países fuera de ella y que son aceptados por la normativa europea.

- Comprobar si los datos se eliminan en el plazo estipulado por la normativa cuando no se trate de los datos que cumplan las condiciones necesarias para ser almacenados más tiempo del que estipula la norma en casos puntuales como sería en caso de que dichos datos deban ser almacenados por un procedimiento legal.

4. Reglamento e-privacy

La Comisión Europea está tratando de que esta norma sea de aplicación a la vez que el RGPD (25 de mayo de 2018)

- Este Reglamento cubre las cookies, además de que regula todas las tecnologías que tratan datos, tanto sin son personales como si no lo son. supone una nueva norma a la que el sector publicitario tendrá que adaptarse.

- El ámbito de aplicación será a los datos de servicios de los usuarios finales que estén situados dentro de la UE, independientemente de la localización de la organización.

- Introduce nuevos conceptos como “metadatos de comunicaciones electrónicas” (que sustituye el concepto de datos de tráfico) y los distingue del concepto de “contenido de las comunicaciones electrónicas”. Establece que estos metadatos se podrán tratar para motivos de seguridad, detectar fallos técnicos y evitar fraude o abuso del servicio, o dar servicios de valor añadido (siempre que se cuente con el consentimiento) y se deberán eliminar o anonimizar cuando se haya llevado a cabo la comunicación, excepto cuando existan motivos legales para mantenerlos.

- Permite a los sitios web que se solicite desactivar el *add-block* para visitar su contenido.

- Establece la necesidad de transparencia e información con avisos destacados sobre el Internet de las cosas en el uso de los datos.

- Comunicaciones comerciales Las comunicaciones comerciales no deseadas (llamadas automáticas, SMS, o email), seguirán requiriendo el consentimiento previo.

- El régimen sancionador establece unas multas similares al del Reglamento Europeo de Protección de Datos de hasta un 4% del volumen de negocios mundial anual o hasta un máximo de 20 millones de euros.

Diferencias RGPD y e-privacy

- El Reglamento de e-privacy se aplica a todos los datos de comunicaciones electrónicas -sean personales o no- e introduce un consentimiento más estricto para la publicidad digital.

- Introduce el término “consentimiento” en el cual al igual que en el RGPD el afectado acepta el tratamiento de sus datos, pero este consentimiento es más complicado de aceptar ya que no siempre se tiene una relación directa con los afectados

Sobre el consentimiento

El nuevo Reglamento propone dejar de lado los avisos informativos de las webs y obtener el consentimiento a través del navegador, eligiendo la configuración de privacidad en la instalación. Sin embargo, los editores (sitios web y aplicaciones) podrían pedir a los usuarios que reconsideren su elección, lo que podría resultar en un aumento de avisos de usuarios intrusos.

5. Tipos de empresas

En primer lugar, se reconocen como empresas privadas todas aquellas que son propiedad de inversores privados, no gubernamentales, accionistas o propietarios (generalmente en conjunto, pero puede ser propiedad de una sola persona), y está en contraste con las instituciones estatales, como empresas públicas y organismos gubernamentales.

Los ficheros de titularidad privada serían los creados con la única finalidad de llevar a cabo la gestión interna del Colegio o Consejo o de adoptar mecanismos que faciliten el desempeño de la profesión colegiada cuando la adopción no implique el ejercicio de potestades administrativas ni lleve aparejada la existencia de un acto administrativo, por ejemplo los relativos a la gestión de recursos humanos del personal que presta sus servicios en el colegio: "Nóminas", "Personal", "Laboral", o los relativos a la gestión contable del colegio: "Facturación", "Clientes", "Proveedores", "Contabilidad", "Suministros".

En cambio, las empresas públicas son empresas propiedad del estado además de aquellas en las que el poder público tenga cierto control sobre este tipo de empresas, dichas empresas tienen objetivos de interés social siendo como ejemplo de empresa de tipo público radio televisión española (RTVE).

Siendo los ficheros de titularidad pública los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades públicas.

Antes de analizar el reglamento cabe destacar el ámbito de aplicación de este reglamento el cual viene dictado en el artículo dos del reglamento de protección de datos el cual establece:

- *La presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.*
- *Esta ley orgánica no* será de aplicación:
    a) *A los tratamientos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*
    b) *A los tratamientos llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito de aplicación del Capítulo II del Título V del Tratado de la Unión Europea.*
    c) *A los tratamientos efectuados por parte de las autoridades competentes y sus agentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención, en los términos previstos por la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por la legislación que la transponga.*
    d) *A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.*
    e) *A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.*
- *Los tratamientos incluidos en el ámbito de aplicación de esta ley orgánica a los que no sea directamente aplicable el Reglamento (UE) 2016/679, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. En particular, el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.*

6. Recogida de los datos del cliente

La recogida de datos del cliente supone el primer momento del tratamiento de los datos, en el reglamento de datos europeo se establecen unas pautas a la hora de tomar los datos de los clientes y el no seguirlas supondría una infracción del reglamento.

- Recogida de datos de personas mayores de dieciocho años.

  En primer lugar, el afectado debe de dar su consentimiento para que se autorice la recogida de los datos además de la finalidad o finalidades de estos, este apartado se refleja en título II, capítulo I, artículo 7 del anteproyecto de la ley orgánica de protección de datos el cual relata.

  Artículo 7. Tratamiento basado en el consentimiento del afectado.

  1. *Se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.*

  2. *Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste claramente dicho consentimiento para cada una de ellas.*

  3. *Cuando en el marco de un proceso de negociación o formalización de un contrato se solicite el consentimiento del afectado para llevar a cabo un tratamiento cuya finalidad no guarde relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá garantizarse que el afectado pueda manifestar específicamente su voluntad en relación con este tratamiento poniendo a su disposición un procedimiento sencillo, claro y comprensible. Este procedimiento podrá consistir, en particular, en la inclusión de una casilla específica en el contrato, siempre y cuando la misma no se encuentre previamente marcada.*

Dicho artículo corresponde al artículo seis, apartado a) del reglamento de datos europeo el cual establece:

Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

Para no quebrantar la aplicación de dichos artículos se deberá de informar al afectado de que se procede a tomar sus datos y la finalidad de dichos datos y que quede constancia de que el afectado está de acuerdo, como, por ejemplo, un documento en el que se describa con claridad que el afectado ha aceptado la toma de sus datos.

También es necesario que si en algún momento posterior a la aceptación del afectado sobre la finalidad de los datos, dicha finalidad cambia, es necesario informar al afectado de dicha finalidad y volver a solicitar la aprobación del afectado para que dichos datos puedan ser utilizados para dicha finalidad.

- Recogida de datos a personas menores de dieciocho años.

  La recogida de datos a personas menores de dieciocho años tiene dos aspectos a tener en cuenta los cuales son reflejados en el título II, capítulo I, artículo 8 del anteproyecto de la ley orgánica de protección de datos el cual dicta:

  Artículo 8. Consentimiento de los menores de edad.

  1. *El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de trece años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.*

  2. *El tratamiento de los datos de los menores de trece años sólo será lícito si consta el consentimiento del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.*

Como se puede comprobar en dicho artículo el consentimiento lo deberá dar el menor con una edad superior a los trece años, salvo cuando la ley exija la asistencia de los titulares o siempre deberá dar el consentimiento los titulares cuando este sea menor de trece años, en cualquier caso, se deberá actuar de dejar constancia de si se aceptan los datos además de su finalidad, y al tratarse de personas menores de dieciocho años se deberá proporcionar dicha solicitud y finalidad en un lenguaje apto para menores de edad.

- Recogida de datos de personas fallecidas

En el caso de que se hayan recogido los datos de una persona y está en el tiempo del tratamiento de los datos fallezca y esta no lo prohíba expresamente, se deberá permitir el acceso y/o supresión de los datos el albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese conferido un mandato expreso.

En caso de menores de edad o personas discapacitadas estas facultades podrán ejercerse, en el marco de sus competencias, por el Ministerio Fiscal.

Este caso está reflejado en el artículo 3 del anteproyecto de la ley orgánica de protección de datos el cual dicta:

Artículo 3. Datos de las personas fallecidas.

1. *Los herederos de una persona fallecida que acrediten debidamente tal condición podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella, y, en su caso, su rectificación o supresión.*

   Como excepción, los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

2. *El albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese conferido un mandato expreso para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste y, en su caso su rectificación o supresión. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.*

3. *En caso de fallecimiento de menores o personas con discapacidad para las que se hubiesen*
   establecido medidas de apoyo, estas facultades podrán ejercerse, en el marco de sus
   competencias, por el Ministerio Fiscal.

- Excepciones de la recogida de datos

  Aunque el afectado dé su consentimiento, no se podrá proceder al tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

  El párrafo anterior hace referencia al artículo 10 del anteproyecto de ley en el cual refleja lo anteriormente citado, además de unos casos concretos donde se puede proceder al tratamiento de los datos anteriormente citados si y solo si son realmente necesarios.

  1. *A los efectos del artículo 9.2 a) del Reglamento (UE) 2016/679, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.*

  2. *Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2. del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, la ley podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, y de los seguros de asistencia sanitaria.*

  Dichos apartados orientados a las empresas privadas expresan en el apartado g) del reglamento europeo que podrán proceder al tratamiento de los datos si dicho tratamiento es necesario por razones de un interés público esencial, que debe ser proporcional al objetivo perseguido. En el apartado e) se trasmite que el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia y en el i) el tratamiento es necesario por razones de interés público en el ámbito de la salud.

También podrán utilizarse de manera licita los datos de una persona que haya manifestado públicamente sus datos personales, estando reflejado en el artículo 13 y dicho artículo no se podrá usar si el afectado es un menor de edad o una persona con discapacidad, dicho artículo expresa:

Artículo 13. Tratamiento de datos hechos manifiestamente públicos por el afectado.

Será lícito el tratamiento de los datos que el propio afectado hubiese hecho manifiestamente públicos siempre y cuando respete los principios establecidos en el artículo 5 del Reglamento (UE) 2016/679, se haya informado al afectado en los términos previstos en el artículo 14 del citado reglamento y se le garantice el ejercicio de sus derechos, en particular los previstos en sus artículos 17 y 19. Lo dispuesto en el párrafo anterior no será de aplicación a los datos de menores de edad o personas con discapacidad para las que se hubiesen establecido medidas de apoyo.

- Recogida de datos personales mediante videovigilancia

Para una empresa privada se podrá hacer uso de la vigilancia siempre y cuando se siga el articulo quince y para la recogida de datos debemos tener en cuenta los apartados primero, segundo y cuarto.

Artículo 15. Tratamientos con fines de videovigilancia.

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Sólo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior. No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte.

3. El deber de información previsto en el artículo 12 del *Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.*

7. Responsable y encargados del tratamiento de los datos

Se define al responsable del fichero o tratamiento como la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados".

Siguiendo el artículo treinta, apartado uno del anteproyecto de ley, el responsable y encargados del mantenimiento tendrán el deber de determinar las medidas técnicas y organizativas para no quebrantar ningún artículo de los reglamentos de protección de datos.

> *Los responsables y encargados, tras ponderar los riesgos que el tratamiento pueda generar en los derechos de los afectados y en particular en su derecho a la protección de datos, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el Reglamento (UE) 2016/679, con la presente ley orgánica, la legislación sectorial y sus normas de desarrollo. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3ª del Capítulo IV del citado reglamento.*

Además, dicho responsable deberá cumplir las siguientes funciones:

Inscripción de ficheros

- Notificar los ficheros ante el Registro General de Protección de Datos, para que se proceda a su inscripción.

Calidad de los datos

- Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.

Deben guardar secreto

- Garantizar el cumplimiento de los deberes de secreto y seguridad.

Deber de información

- Informar a los titulares de los datos personales en la recogida de éstos.
- Obtener el consentimiento para el tratamiento de los datos personales.

Atención de los derechos de los ciudadanos

- Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En primer lugar, en la empresa deberemos asignar uno o más encargados del tratamiento para el cual tendremos que seguir el artículo treinta y cuatro del anteproyecto de ley que dicta:

Artículo 34. Encargado del tratamiento.

1. *El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.*

2. *Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.*

3. *El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos de carácter personal deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.*

4. *El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento. 5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la 40 Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.*

En segundo lugar, en la empresa podrán haber más de un responsable del tratamiento, en cuyo caso seguirán el articulo treinta y uno del anteproyecto de ley que dicta:

Artículo 31. Supuestos de corresponsabilidad en el tratamiento.

1. *La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.*

2. *Cuando una norma con rango de ley establezca una habilitación legal para el tratamiento de datos de carácter personal conforme a lo dispuesto en el artículo 9.3 de esta ley orgánica, previendo que varias entidades sean corresponsables del tratamiento, podrá fijar las funciones y relaciones respectivas de los corresponsables en relación con los afectados a los efectos previstos en el artículo 26.2 del Reglamento (UE) 2016/679.*

Dichos responsables y encargados del tratamiento tendrán la obligación de llevar un registro del tratamiento de los datos para así poder cumplir el articulo treinta y tres el cual consta en:

Artículo 33. Registro de las actividades de tratamiento.

1. *Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5. El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.*

2. *Los sujetos enumerados en el artículo 77.1 harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.*

En el caso en el que la empresa tenga responsables y encargados del tratamiento fuera de la unión europea, deberemos seguir el artículo treinta y dos.

Artículo 32. Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea.

1. *En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679. Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.*

2. *Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.*

Si la empresa cumple alguna de las condiciones que se detallan a continuación, también deberemos asignar un delegado de protección de datos siguiendo el artículo treinta y siete, apartado uno del reglamento de datos europeo el cual establece:

Designación del delegado de protección de datos 1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

1) *el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.*
2) *las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.*
3) *las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.*

Además de estas condiciones el anteproyecto de ley refleja las siguientes condiciones en el artículo treinta y cinco.

1) *colegios profesionales y sus consejos generales regulados por la Ley 2/1974 de 13 febrero, sobre colegios profesionales.*
2) *Los centros docentes que ofrezcan enseñanzas reguladas por la Ley Orgánica 2/2006 de 3 de mayo, de Educación, y las Universidades públicas y privadas.*
3) *Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en la Ley 9/2014, de 9 de mayo, General de telecomunicaciones.*
4) *Los prestadores de servicios de la sociedad de la información que recaben información de los usuarios de sus servicios.*
5) *Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.*
6) *Los establecimientos financieros de crédito.*
7) *Las entidades aseguradoras y reaseguradoras sometidas a la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.*
8) *Las empresas de servicios de inversión, reguladas por el Título V del texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.*
9) *Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada que podrán designar un delegado de protección de datos voluntario.*

En el caso en el que la empresa deba tener asignado un delegado de protección de datos este deberá debidamente cualificado para así no quebrantar el artículo treinta y seis el cual establece:

Artículo 36. Cualificación del delegado de protección de datos.

El delegado de protección de datos sea una persona física o jurídica, deberá reunir los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 y demostrar reconocida competencia en la materia. Los requisitos podrán acreditarse por los medios correspondientes, incluidos los mecanismos de certificación.

Como dicho delegado deberá cumplir unas funciones que incluso podrían llevar a perjudicar a la empresa dicho delegado está protegido por el artículo treinta y siete el cual nos dictamina la posición del delegado en la empresa y de los derechos que este tiene. Dicho artículo dicta lo siguiente:

Artículo 37. Posición del delegado de protección de datos.

1) *El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos.*

2) *Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio.*

3) *El responsable y el encargado del tratamiento pondrán a disposición del delegado de protección de datos los medios materiales y personales que resulten precisos para el adecuado desempeño de sus funciones, asignándole cuando proceda personal subordinado, así como locales, instalaciones y equipos.*

4) *En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 6 de esta ley orgánica.*

5) *Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento, proponiéndoles las medidas necesarias para evitar la persistencia en esa conducta.*

8. Tratamiento de los datos

El reglamento europeo define el tratamiento de datos siguiendo *el artículo cinco Principios relativos al tratamiento:*

1. *Los datos personales serán:*

    a. *tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);*

    b. *recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);*

    c. *adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);*

    d. *exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); 4.5.2016 ES Diario Oficial de la Unión Europea L 119/35 (1) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).*

    e. *mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);*

f. tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. *El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).*

Es decir, y utilizando la definición del reglamento de la ley orgánica de protección de datos, el real decreto 1720/2007 mostrada en la página web http://www.cuidatusdatos.com/infotratamiento.html el tratamiento de datos consiste en:

> *"Toda operación y procedimiento de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."*

Continuando con nuestro flujo de los datos donde, estos son recogidos siguiendo los artículos correspondientes del reglamento explicados anteriormente y siguiendo las medidas de seguridad correspondientes para su almacenamiento, vamos a continuar explicando cómo deben de tratarse los datos para no quebrantar ningún artículo del reglamento.

En primer lugar, todo tipo de datos que se traten deben ser exactos y siguiendo el artículo cinco todo dato proveniente del afectado se asumirá como exacto tal y como dicta el propio artículo:

> *"Artículo 5. Presunción de exactitud.*
>
> *A los efectos previstos en el artículo 5.1 d) del Reglamento (UE) 2016/679, se presumirán exactos y actualizados los datos obtenidos directamente del afectado."*

El artículo del reglamento europeo que referencia nos dicta que en caso de que no sean exactos se deben de poder de modificar si el afectado comunica que sus datos no son exactos:

> *"Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan."*

En segundo lugar, para no quebrantar el artículo seis, toda persona que trabaje en el tratamiento de los datos deberá guardar confidencialidad:

> *Artículo 6. Deber de confidencialidad.*
>
> 1. *Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de éste estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1 f) del Reglamento (UE) 2016/679.*
>
> 2. *La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.*
>
> 3. *Las obligaciones establecidas en los apartados anteriores se mantendrán con carácter indefinido, aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.*

Cabría destacar en el caso en el que la empresa sea de tipo **público**, la importancia del artículo nueve *Tratamiento de datos amparado por la ley* el cual establece:

1. *El tratamiento de datos de carácter personal sólo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1 c) del Reglamento (UE) 2016/679, cuando así lo prevea una ley, que deberá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. La ley podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el Capítulo IV del Reglamento (UE) 2016/679.*

2. *El tratamiento de datos de carácter personal sólo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por la ley.*

3. *3. La ley podrá considerar fundado un determinado tratamiento en la concurrencia de un interés legítimo del responsable del tratamiento o de un tercero que prevalece sobre los derechos del afectado, en los términos previstos en el artículo 6.1 f) del Reglamento (UE) 2016/679. En estos supuestos, la ley podrá exigir al responsable la adopción garantías adicionales. Lo dispuesto en el párrafo anterior no impide que el tratamiento de datos personales pueda considerarse lícito al amparo del artículo 6.1 f) del Reglamento (UE) 2016/679, aun cuando no exista una previsión legal específica.*

En tercer lugar, tendremos que tener muy en cuenta el artículo diez el cual trata sobre las categorías especiales de datos y nos indican que tipos de datos debemos tratar siendo este muy importante ya que, aunque el afectado nos de su consentimiento, quebrantaríamos el artículo diez el cual establece:

Artículo 10. Categorías especiales de datos.

1. *A los efectos del artículo 9.2 a) del Reglamento (UE) 2016/679, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.*

2. *Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2. del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.*

En particular, la ley podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, y de los seguros de asistencia sanitaria.

Como se puede extraer del reglamento de datos europeo, artículo nueve, apartado dos:

> *Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física menos en los casos:*
>
> *g) El tratamiento es necesario por razones de un interés público esencial, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.*
>
> *h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.*
>
> *i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.*

En el artículo cinco se menciona que el tratamiento de los datos debe ser licito y en el artículo once que hace referencia al artículo seis del reglamento europeo del cual extraemos la siguiente información:

Será lícito si se cumple al menos una de las siguientes condiciones:

- *El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.*
- *El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte.*
- *El tratamiento es necesario para el cumplimiento de una obligación legal.*
- *El tratamiento es necesario para proteger intereses vitales del interesado.*
- *El tratamiento es necesario para el cumplimiento de una misión realizada en interés público.*
- *el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño, pero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.*

Los Estados miembros podrán mantener o introducir disposiciones más específicas para los apartados 3º y 5º anteriormente descritos.

La base del tratamiento de estos 2 apartados deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica y podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento.

Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

- *Si existe algún tipo de relación entre el fin que consintió el afectado y el fin que se hace sin su consentimiento.*
- *El contexto en que se hayan recogido los datos personales.*
- *La naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales.*
- *Las posibles consecuencias para los interesados.*

- *la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.*

Si la empresa mantiene datos de contacto con el afectado, deberá tener en cuenta que puede quebrantar el artículo doce

Artículo 12. Tratamiento de datos de contacto y de empresarios individuales.

1. *Se entenderá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:*

   a) Que el tratamiento se refiera únicamente a los mínimos datos imprescindibles para su localización profesional.

   b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. *El mismo amparo legal tendrá el tratamiento de los datos relativos a los empresarios individuales cuando se refieran a ellos en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.*

El artículo seis, apartado uno, subapartado f indica:

"el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."

En esta época en el que una gran mayoría de gente publica sus datos personales en Internet, se podría dar por hecho de que se podría utilizar los datos de manera licita al ser estos públicos para todo el mundo, pero lo cierto es que el artículo trece nos da indicaciones sobre la licitud de los datos hechos públicos por el afectado siendo estos no aplicables a menores de edad y personas con discapacidad:

> *Artículo 13. Tratamiento de datos hechos manifiestamente públicos por el afectado.*
>
> *Será lícito el tratamiento de los datos que el propio afectado hubiese hecho manifiestamente públicos siempre y cuando respete los principios establecidos en el artículo 5 del Reglamento (UE) 2016/679, se haya informado al afectado en los términos previstos en el artículo 14 del citado reglamento y se le garantice el ejercicio de sus derechos, en particular los previstos en sus artículos 17 y 19. Lo dispuesto en el párrafo anterior no será de aplicación a los datos de menores de edad o personas con discapacidad para las que se hubiesen establecido medidas de apoyo.*

Si la empresa debe tratar datos de tipo crediticio debemos de tener en cuenta el artículo catorce del reglamento del cual se ha extraído lo siguiente:

Artículo 14. Sistemas de información crediticia.

Será licito el tratamiento de datos relativos al incumplimiento de obligaciones dinerarias, financieras por sistemas comunes de información crediticia cuando:

- *datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.*
- *Que los datos se refieran a deudas ciertas, vencidas y exigibles que no sean objeto de reclamación judicial*
- *Que el acreedor informe al posible afectado de que se puede ser incluido en dichos sistemas*
- *Que el acreedor haya requerido previamente de pago al deudor, advirtiéndole de su posible inclusión en el sistema.*

La entidad que mantenga el sistema deberá notificar al afectado de la inclusión de sus datos, así como de notificarle la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 y dicho sistema no podrá utilizar los datos durante 30 días siguientes a la notificación de la deuda.

También será licito cuando:

- *Siempre y cuando el afectado hubiere dado su consentimiento al tratamiento de dichos datos.*
- *Si en el sistema se incluyesen datos relativos tanto a cumplimientos como a incumplimientos sólo será necesario el consentimiento respecto de los primeros.*

Los sistemas deberán seguir las siguientes normas:

- *Los datos relativos al cumplimiento sólo podrán mantenerse en el sistema durante un período de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.*
- *Los datos relativos al incumplimiento permanecerán en el fichero sin consentimiento del interesado en tanto persista el incumplimiento.*
- *La extinción de la deuda y, en particular, su pago o cumplimiento implicarán la supresión inmediata de los datos de los sistemas*
- *los datos relativos al pago podrán ser incorporados a los sistemas referidos al cumplimiento de dichas obligaciones si el interesado hubiera prestado su consentimiento para ello*
- *Los datos referidos a un deudor determinado podrán ser consultados en los supuestos previstos en la Ley 16/2011*
- *Las entidades que mantengan el sistema y las acreedoras tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.*
- *El presente artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales relacionadas con el deudor 27 y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.*

Siguiendo el orden de los artículos del anteproyecto de ley, llegamos al artículo 15 el cual trata de un tema muy importante que se refiere al tratamiento con fines de videovigilancia del cual se ha extraído lo siguiente:

Artículo 15. Tratamientos con fines de videovigilancia.

- *Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.*

- *Sólo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para preservar dicha seguridad.*

- *Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos.*

- *No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 29.*

- *Para cumplir el artículo 12 del reglamento (UE) 2016/679 se deberá indicar la existencia de dicha vigilancia y al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679.*

- *Los empleadores podrán tratar los datos obtenidos a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del Estatuto de los Trabajadores siempre que les hubieran informado acerca de esta medida.*

- *Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento de imágenes en el propio domicilio del encargado.*

- *El tratamiento de los datos personales procedentes de las imágenes y sonidos se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.*

- *Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada.*

Artículo 16. Sistemas de exclusión publicitaria.

1. Será lícito el tratamiento de datos de carácter personal que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas. A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que sólo se incluirán los datos imprescindibles para identificar a los afectados.

2. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados con fines de publicidad o prospección comercial, éste deberá informarle de los sistemas de exclusión publicitaria existentes, identificando a su responsable.

3. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo.

4. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán su creación, su carácter general o sectorial y el modo en que los afectados pueden incorporarse a los mismos a la Agencia Española de Protección de Datos, que hará pública la citada información.

Artículo 17. Sistemas de información de denuncias internas en el sector privado.

1. Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad privada, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.

2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente al personal que lleve a cabo las funciones de control interno y de cumplimiento de la entidad y, sólo cuando procediera la adopción de medidas disciplinarias contra un trabajador, al personal con funciones de gestión y control de recursos humanos.

3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a la persona que hubiera puesto los hechos en conocimiento de la entidad si se hubiera identificado.

4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema únicamente durante el tiempo imprescindible para la averiguación de los hechos denunciados. En todo caso, transcurridos tres meses desde la introducción de los datos deberá procederse a su supresión del sistema. Si fuera necesaria su conservación para continuar la investigación podrán seguir siendo tratados en un entorno distinto. No será de aplicación a estos sistemas la obligación de bloqueo prevista en el artículo 29.

Artículo 18. Tratamientos relacionados con la realización de determinadas operaciones mercantiles.

Serán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

Artículo 19. Tratamiento de datos en el ámbito de la función estadística pública.

1. El tratamiento de datos de carácter personal llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en la Ley 12/1989, de 9 de mayo, reguladora de la Función estadística pública y la normativa autonómica que resulte en su caso de aplicación y a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística sólo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos. De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, sólo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 exclusivamente cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica. 31

Artículo 20. Tratamiento de datos de naturaleza penal.

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, sólo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. Corresponde al Ministerio de Justicia la gestión de los sistemas de información en que se recoja la totalidad de los datos relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas.

9. Seguridad de los datos

A lo largo del anteproyecto de ley y en especial en el artículo nueve del anteproyecto de ley nos informan que se deben de tomar las medidas de seguridad apropiadas u otras medidas de seguridad adicionales cuando la empresa trate con categorías de datos especiales y en este apartado se procede a explicar en qué consisten dichas medidas de seguridad, pero primero cabe destacar el propio artículo nueve del anteproyecto de ley.

Artículo 9. Tratamiento de datos amparado por la ley.

1. El tratamiento de datos de carácter personal sólo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1 c) del Reglamento (UE) 2016/679, cuando así lo prevea una ley, que deberá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. La ley podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el Capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos de carácter personal sólo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por la ley.

3. La ley podrá considerar fundado un determinado tratamiento en la concurrencia de un interés legítimo del responsable del tratamiento o de un tercero que prevalece sobre los derechos del afectado, en los términos previstos en el artículo 6.1 f) del Reglamento (UE) 2016/679. En estos supuestos, la ley podrá exigir al responsable la adopción garantías adicionales. Lo dispuesto en el párrafo anterior no impide que el tratamiento de datos personales pueda considerarse lícito al amparo del artículo 6.1 f) del Reglamento (UE) 2016/679, aun cuando no exista una previsión legal específica.

- El reglamento dicta que la información debe ser guardada en ficheros y tal como se define el concepto de fichero en la página web de la agencia española de protección de datos un fichero es**:**

  "todo conjunto organizado de datos de carácter personal, permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso."

Sobre la cantidad de ficheros que el reglamento indica nos ofrece dos opciones siendo ambas perfectamente válidas mientras se cumplan las medidas de seguridad apropiadas para el tipo de datos que se deban tratar, estas opciones son:

1. Un solo documento que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable.

2. Un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido.

Sea cual sea la opción que la empresa haya elegido la empresa tendrá que tener las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos del reglamento que se muestran a continuación por apartados.

También será necesario que la empresa tenga en cuenta que dependiendo del tipo de datos que se traten, se deberá adoptar unas medidas de seguridad más exigentes, estos niveles de seguridad son:

- Nivel alto

  "Ficheros o tratamientos con datos: de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico; recabados con fines policiales sin consentimiento de las personas afectadas; y derivados de actos de violencia de género."

- NIVEL MEDIO
  "Ficheros o tratamientos con datos: relativos a la comisión de infracciones administrativas o penales; que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito); de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias; de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros; de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias; de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; 8 que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización."

- NIVEL BÁSICO
  "Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando: los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros; se trate de ficheros o tratamientos de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos."

Siendo muy importante recalcar que un dato que requiera un nivel de seguridad alto deberá incluir las medidas de seguridad de un nivel básico y un nivel medio además de las medidas de seguridad pertinentes de un nivel alto. De misma forma unos datos con nivel de seguridad medio deberán incluir las medidas de seguridad de un nivel básico y las medidas del nivel medio.

Identificación y autenticación

La identificación de los usuarios se deberá hacer de forma personalizada e impidiendo que usuarios no autorizados al acceso de los ficheros puedan acceder a su contenido, por este motivo si la autentificación se realiza por contraseña la empresa deberá determinar la longitud en caracteres de la contraseña, el uso de caracteres no alfanuméricos, mayúsculas y por supuesto la periodicidad con la que la contraseña deba ser cambiada.

Control de acceso

Para no cometer infracciones en el control de acceso, los usuarios deberán de tener los permisos apropiados para acceder a los ficheros necesarios para el desarrollo de sus funciones, siendo la excepción la persona encargada de dar los permisos al resto de trabajadores.

También es necesario que la empresa deje constancia de cuál es el procedimiento para que un usuario solicite el alta para tener permisos para poder acceder a un documento con los datos personales que deba tratar, además de también de dar de baja usuarios que dejen de trabajar en dicho fichero al haberse finalizado el tratamiento o por que el trabajador ya no trabaja en la empresa y ya no deba de tener ningún tipo de acceso a los ficheros.

Registro de accesos

Este apartado es necesario cuando el tipo de datos que se tratan en un fichero requieren un tipo de tratamiento especial y una seguridad más elevada, siendo esta medida un procedimiento automatizado o seguido por un control exhaustivo que consistirá en el almacenamiento de la persona, la fecha y la hora en la que el usuario accede al documento siendo este proceso revisado por un responsable de seguridad.

Este control de acceso podrá evitarse, siempre que el responsable del fichero sea una persona física, se dé la garantía de que solo el responsable del fichero acceda y trate los datos. También deberá conservarse el registro de acceso un mínimo de dos años dando libertad para guardar el fichero on-line u offline.

Manuales

El acceso a la documentación se limita exclusivamente al personal autorizado.

Gestión de soportes y documentos

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en un lugar de acceso restringido al que solo tendrán acceso las personas con autorización, salvo que, por cuestiones físicas, estos no puedan ser inventariados y almacenados.

Los soportes que la empresa opte por tratar con unas medidas de seguridad más elevadas debido a datos que contengan se podrán identificar utilizando sistemas de etiquetado que la empresa considere oportunos pero que sean comprensibles para usuarios identificados pero que dificulten su comprensión a usuarios no identificados.

El inventario de soportes puede anexarse al documento o gestionarse de forma automatizada, en este último caso se indicará en este punto el sistema informático utilizado.

En el caso en el que la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo con el siguiente procedimiento.

También cabe destacar que los soportes y documentos que vayan a ser trasladados deberán de seguir el procedimiento de la empresa con el objetivo de evitar la pérdida o sustracción de información. De igual manera los soportes y documentos desechados, deberán ser eliminados siguiendo el procedimiento que la empresa defina.

Si dicha gestión de soportes y documentos se realiza de manera automatizada y además los datos deben tomar las medidas de seguridad de nivel medio o nivel alto, se deberán tomar las siguientes medidas:

- Nivel medio

  Las salidas y entradas de soportes correspondientes a los ficheros de nivel medio y alto, serán registradas de acuerdo con el procedimiento que la empresa detalle.

  - Para las entradas como mínimo:

  El tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción.

  - Para las salidas como mínimo:

  El tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega.

- Nivel alto

  Además de las medidas de registro del nivel medio, también se deberá de seguir una gestión y distribución de soporte apropiada, para el cual En este caso los soportes se identificarán mediante el sistema de etiquetado comprensibles y con significado para los usuarios con acceso autorizados, permitiéndoles identificar su contenido y dificultando la identificación para el resto de las personas.

  En cuanto a La distribución y salida de soportes que contengan datos de carácter personal de los ficheros de nivel alto se realizará mediante un cifrado que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Igualmente se cifrarán los datos que contengan los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable. Tomando las medidas alternativas oportunas cuando en un dispositivo portátil no se permita el cifrado de los datos personales.

Sobre los manuales relacionados con la gestión de soportes y documentos deberán seguir las medidas apropiadas para los siguientes apartados:

- Criterios de archivo.

  Manual con todo lo necesario para garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitarán el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

- Almacenamiento de la información.

  Manual en el que se indica la manera y el lugar de almacenamiento de la información que deberá incluir las medidas de acceso para evitar que personas no autorizadas puedan acceder a los datos.

  Si el tipo de datos que se almacenan requieren un nivel de seguridad alto, y se tratan de material físico que deba guardarse en armarios, archivadores u otros elementos físicos, estos deberán estar cerrados bajo llave y siempre cerrados excepto cuando se tenga que acceder a los documentos, si esto no fuera posible, debería indicarse en el manual que medidas alternativas se toman.

- Custodia de soportes.

  Mientras están en tramitación los puntos anteriores, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones sean o no públicas, garantizarán un nivel de seguridad equivalente al exigido para los accesos en modo local, además si se realiza de manera automatizada y corresponde a un nivel de seguridad alto se deberán realizar un cifrado de los datos que garanticen que no sea legible y/o manipulada por terceros.

Régimen de trabajo fuera de los locales de la ubicación del fichero

Se pueden llevar a cabo el tratamiento de datos personales fuera del local donde se ubica el responsable del fichero, para poder realizar está acción deberán detallarse donde están los locales a donde se desea llevar los tratamientos, además de los ficheros que se van a trasladar y deberán ser realizados por personas autorizadas y que cumplan los procedimientos de seguridad impuestos por la empresa.

Manuales necesarios para un de nivel de seguridad alto

- Traslado de documentación

  En este manual se incluirán las medidas necesarias o medidas alternativas para el traslado físico de documentación

- Ficheros temporales o copias de trabajo de documentos

  Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que haya dejado de ser necesarios para los fines que motivaron su creación.

- Copia o reproducción

  En este manual se incluye el personal o perfiles autorizados a la realización de las copias de reproducción y una vez desechadas deberán ser correctamente destruidas además de garantizar el correcto acceso a los documentos originales.

- Copias de respaldo y recuperación

  Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos como mínimo una vez a la semana, dichas copias de respaldo deberán garantizar la correcta reconstrucción del documento original, en caso de documentos parcialmente automatizados se deberán grabar los datos manualmente los datos, siendo tarea del responsable del fichero la verificación semestral de los procedimientos.

  En caso de que estemos tratando un documento con una seguridad necesaria de nivel alto además deberemos conservar una copia de respaldo y otra copia de los procedimientos de recuperación de datos dicha copia deberá estar en un lugar físico diferente al documento original o utilizando elementos que garanticen la recuperación de la información que sea recuperable.

- Responsable de seguridad también necesario para un nivel de seguridad medio

  Deberá de haber un responsable de seguridad encargado de controlar la correcta aplicación de las medidas de seguridad en el documento.

Información y obligaciones del personal

La empresa deberá de informar al personal de la misma de las normas de seguridad de la misma y deberá realizarse un procedimiento sobre dicha información diferenciándola en función de los perfiles además de incluir las consecuencias de no seguir las normas de seguridad.

Funciones y obligaciones del personal

Un miembro de la empresa tendrás que cumplir las siguientes obligaciones:

1. Notificar de las incidencias de seguridad de las que se tenga conocimiento
2. Guardar confidencialidad sobre los datos personales que conozcan en el entorno de trabajo.
3. Cumplir las obligaciones de los perfiles a los que pertenecen.
4. No acceder a datos donde no tienen acceso.
5. Informar al personal ajeno de la prohibición de acceder a datos personales y la obligación de guardar secreto de los que hayan conocido durante su servicio.

Procedimientos de notificación, gestión y respuesta ante las incidencias

En el documento de procedimientos deberán incluirse todos los procedimientos en caso de incidencia, donde debe incluirse todo lo necesario para dar una respuesta a la incidencia lo más ágil posible, es decir, a quien debe notificar el empleado que vea la incidencia y de qué modo gestionarla.

También deberá incluir los procedimientos para poder registrar la incidencia donde será necesario que conste el tipo de incidencia, hora, la persona que la ha detectado y a quien notificó.

En el caso en el que el procedimiento sea automatizado y los datos necesiten un nivel de seguridad medio o alto, también se incluirá donde poder encontrar los procedimientos de recuperación, siendo necesaria la autorización por escrito del responsable del fichero.

Procedimientos de revisión

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios que pudieran repercutir en el cumplimento de las medidas de seguridad en el sistema de información.

En este apartado se especificará los procedimientos para modificar el documento de seguridad, por supuesto especificando quien puedo proponer y aprobar los cambios además de al personal que deben informar una vez realizados los cambios.

Además, en un nivel medio o alto de seguridad deberán incluirse los procedimientos para realizar la auditoría de seguridad de la empresa como mínimo cada dos años, para el cual puede observarse los puntos que se analizan en este documento y comprobar si cumplen todas las medidas necesarias para el cumplimiento del anteproyecto de ley de protección de datos.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas.

Por último, en el apartado de seguridad, si los datos requieren un nivel alto de seguridad, aparte de la auditoria también se deberá realizar un informa mensual sobre el registro de accesos, para el cual se deberá indicar los procedimientos para la realización del informe mensual.

10. Códigos de conducta/tipo

Las empresas podrán aplicar códigos de conducta/tipo, los cuales no son obligatorios pero una empresa puede adoptar los códigos de conducta que la Agencia Española de Protección de Datos ofrece a sus consumidores. Además, una empresa podrá diseñar un código de conducta y registrarlo en Registro General de Protección de Datos y si resulta aprobado por la Agencia Española de Protección de Datos podrán aplicarlos dentro de la empresa, dichos códigos de conducta están regulados por el artículo treinta y nueve del anteproyecto de ley que dicta:

Artículo 39. Códigos de conducta.

1. Los códigos de conducta regulados por la Sección 5ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas, así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

3. Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679. En este supuesto, los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 38 de esta ley orgánica. En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

4. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente. En el supuesto al que se refiere el apartado 3 de este artículo la autoridad de protección de datos competente verificará previamente que los organismos o entidades que lo promuevan reúnen los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

5. La Agencia Española de Protección de Datos someterá los proyectos de código al procedimiento previsto en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos que procedan según su artículo 40.7. El procedimiento quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen al que se refiere el artículo 64.1.b) del citado reglamento.

6. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán un registro de los códigos de conducta aprobados por las mismas y los aprobados conforme al artículo 63 del Reglamento (UE) 2016/679. El registro será accesible a través de medios electrónicos.

7. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Como se puede observar en el artículo treinta y nueve, este hace referencia a los siguientes apartados del reglamento europeo de protección de datos:

- Artículo cuarenta, apartado dos

  Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

  a) el tratamiento leal y transparente; L 119/56 ES Diario Oficial de la Unión Europea 4.5.2016.

  b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

  c) la recogida de datos personales.

  d) la seudonimización de datos personales.

  e) la información proporcionada al público y a los interesados.

  f) el ejercicio de los derechos de los interesados.

  g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño.

  h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32.

  i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados.

  j) la transferencia de datos personales a terceros países u organizaciones internacionales.

  k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

- Artículo cuarenta y uno

Supervisión de códigos de conducta aprobados

1. *Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.*

2. *El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:*

    a. *ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código.*

    b. *ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación.*

    c. *ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público.*

    d. *ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.*

3. *La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los criterios de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.*

4. *Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.*

5. *La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento. 6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.*

- Artículo sesenta y tres

  Mecanismo de coherencia

  A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

- Artículo sesenta y cuatro, apartado uno

  Dictamen del Comité 1.

  El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

  a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

  b) b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento; 4.5.2016 ES Diario Oficial de la Unión Europea L 119/73

  c) c) tenga por objeto aprobar los criterios aplicables a la acreditación de un organismo con arreglo al artículo 41, apartado 3, o un organismo de certificación conforme al artículo 43, apartado 3.

  d) d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8.

  e) e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a).

  f) f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.

Aspectos formales de la solicitud de inscripción de los códigos tipo y procedimiento de Inscripción

La solicitud, que deberá reunir los requisitos legalmente establecidos (artículos 54 y 66 de la Ley 39/2015), habrá de acompañarse de los siguientes documentos:

- Acreditación de la representación que concurra en la persona que presente la solicitud.
- Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.
- En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó, así como copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.
- Para los códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.
- En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.
- El propio código tipo sometido a la Agencia Española de Protección de Datos.

Tramitación de la solicitud:

- Durante los treinta días siguientes a la presentación de la solicitud o, en su caso, subsanación de los defectos advertidos, se podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

- Informe del RGPD sobre las características del proyecto de código tipo, y remisión al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII del Reglamento.

- Información pública (trámite potestativo).

- En cualquier fase del procedimiento se podrá requerir al solicitante para que complete o modifique la documentación presentada en el plazo de 30 días, plazo para el que se declarará la suspensión del procedimiento.

Concluidos los trámites previstos del procedimiento, el director de la Agencia resolverá sobre la inscripción del código tipo en el Registro General de Protección de Datos.

Obligaciones de las entidades promotoras de los códigos tipo (art. 78 RLOPD)

- Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos referida anteriormente. Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

- Elaborar y remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

- Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento. La evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

Favorecer la accesibilidad de las personas que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

Como ejemplo de un código de conducta o tipo la Agencia Española de Protección de datos nos ofrece una colección de códigos de conducta para que podamos aplicarlos a la empresa si deseamos, dicha página se encuentra en la siguiente ubicación:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php

O en caso de que el enlace no funcione se puede consultar en la página oficial de la Agencia Española de Protección de Datos, una vez dentro accederíamos al canal de responsable y en el apartado códigos de conducta podremos acceder la información relevante sobre los códigos de conducta y un repositorio para consultarlo. Como ejemplo para una empresa privada sobre seguros de automóvil la Agencia Española de Protección de datos nos propone el siguiente documento: https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/pdfs/CODIGO_TIPO_DE_FICHERO_HISTORICO_DE_SEGUROS_DEL_AUTOMOVIL-UNESPA-2017.pdf

Este documento corresponde al código de conducta para una empresa dedicada a seguros de automóvil el cual nos ofrece el número de código de inscripción al registro, la fecha de inscripción al registro y la fecha de adecuación al registro, además de que también nos facilitan la resolución de la inscripción de cómo fue aceptado en el registro
https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/resoluciones/CT-0002-2000_Resolucion_16_11_2009.pdf

11. Derechos de los afectados

Una de las principales novedades del anteproyecto de ley es el derecho que tendrán los afectados para acceder a sus propios datos, solicitar la modificación de sus datos para que estos cumplan con la obligación de exactitud, también para el derecho de oponerse a la toma de datos y por supuesto para solicitar la eliminación de sus datos o el bloqueo a sus datos personales. Esta novedosa incorporación de derechos que la Agencia Española de protección de datos personales debe implantar en el próximo reglamento que entrará en validez el día veinticinco de mayo de 2018 para así poder cumplir el reglamento de datos europeo que siguen todos los países de la unión europea.

Pero antes de comenzar con los derechos de los afectados, cabe destacar el artículo veinte y dos del anteproyecto de ley el cual establece:

Artículo 22. Disposiciones generales sobre ejercicio de los derechos.

1. *Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.*

2. *La identidad del afectado y, en su caso, la de su representante deberá acreditarse mediante documento válido, incluido aquel que permita su identificación electrónica.*

3. *El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.*

4. *El encargado podrá atender, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.*

5. *La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.*

6. *Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquéllas.*

Como podemos ver en el artículo número veintidós, las empresas deberán de facilitar a los afectados una manera accesible para poder ejercer sus derechos, si la empresa no presta atención en el tema y no ofrece accesibilidad a los afectados, la empresa podría enfrentarse una infracción con sanción económica.

Derecho de acceso

El derecho de un afectado a acceder a los datos de los que pertenece el afectado es un derecho reflejado en el artículo veintitrés el cual dicta lo siguiente:

1. *El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679. Cuando el responsable trate una gran cantidad de información relativa al afectado y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.*

2. *El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. La comunicación del sistema al afectado permitirá denegar su solicitud de acceso.*

3. *Cuando el afectado elija un medio distinto al que se le ofrece asumirá los riesgos y los costes desproporcionados que su elección comporte.*

4. *A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.*

Pero tras leer el artículo veintidós la empresa puede tener duda de que datos son los que deben ser accesibles por el cliente y esto se ve reflejado en el artículo quince del reglamento europeo del cual se ha extraído lo siguiente:

- los fines del tratamiento.
- las categorías de datos personales de que se trate.
- los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales.
- de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.
- la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento.
- el derecho a presentar una reclamación ante una autoridad de control.
- cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
- la existencia de decisiones automatizadas, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas.

- El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos.

Y el artículo 12.5 sobre considerar un comportamiento de carácter repetitivo:

Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:
cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Derecho de rectificación

El derecho de rectificación es un derecho disponible por el afectado el cual puede solicitar la corrección de unos datos erróneos o desactualizados, este derecho se ve representado en el artículo veinticuatro el cual establece:

Artículo 24. Derecho de rectificación.

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Dicho artículo que se referencia en el reglamento europeo de protección de datos nos indica*:*

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Derecho de supresión

Es el derecho del afectado a solicitar la eliminación de sus datos y está regulado según el artículo veinticinco de anteproyecto de ley.

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679. 2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2

2. del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Siendo las referencias del artículo veinticinco, las correspondientes a los artículos diecisiete y veintiuno, apartado dos que dictan lo siguiente:

Artículo 17 Derecho de supresión («el derecho al olvido»)

1. *El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*
    a. *los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; 4.5.2016 ES Diario Oficial de la Unión Europea L 119/43*
    b. *el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;*
    c. *el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;*
    d. *los datos personales hayan sido tratados ilícitamente;*
    e. *los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;*
    f. *los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.*
2. *Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.*

3. *Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:*
   a) *para ejercer el derecho a la libertad de expresión e información;*
   b) *para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;*
   c) *por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones.*

El artículo veintiuno, apartado dos dicta:

El artículo 21.2 dice:

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Derecho a la limitación del tratamiento.

1. *El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.*

2. *El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en el sistema.*

Siendo las condiciones para que el afectado pueda ejercer este derecho, las descritas en el artículo dieciocho del reglamento de datos europeos el cual establece:

1. *El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:*

   a. *el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.*

   b. *el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;*

   c. *el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;*

d. *el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.*

2. *Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. L 119/44 ES Diario Oficial de la Unión Europea 4.5.2016*

3. *Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.*

Derecho a la portabilidad.

Representado en el artículo veintisiete, que dicta lo siguiente:

1. *El derecho a la portabilidad regulado en el artículo 20 del Reglamento (UE) 2016/679 podrá ejercerse por el afectado respecto de los datos que hubiera facilitado al responsable del tratamiento y de los que se deriven directamente del uso por aquél de los servicios prestados por el responsable.*

2. *El derecho a la portabilidad no se extenderá a los datos que el responsable hubiere inferido a partir de aquellos a los que se refiere el apartado anterior. En todo caso, el afectado podrá ejercer respecto de estos datos los restantes derechos enumerados en este capítulo, particularmente el derecho de acceso contemplado en el artículo 15 del Reglamento (UE) 2016/679.*

En el reglamento de datos europeo el artículo que es referenciando dicta lo siguiente:

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Derecho de oposición

El derecho de oposición se ve representado en el artículo veintiocho el cual establece:

> *El derecho de oposición se ejercerá de acuerdo con lo establecido en el artículo 21 del Reglamento (UE) 2016/679.*

Dicho artículo veintiuno referenciado en el artículo veintiocho del anteproyecto de ley dicta lo siguiente:

1. *El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.*

2. *Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.*

3. *Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines. 4.5.2016 ES Diario Oficial de la Unión Europea L 119/45.*

4. *A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.*

5. *En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.*

6. *Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.*

12. Transferencias internacionales de datos

Si la empresa transfiere datos internacionalmente, deberemos de tener en cuenta los artículos que se detallan a continuación a fin de no quebrar ningún artículo del anteproyecto de ley o del reglamento europeo de datos, ya que la empresa podría cometer una infracción grave. En el anteproyecto de ley, el artículo cuarenta y uno nos dicta que el apartado de transferencias internacionales de datos se hará siguiendo el reglamento europeo de protección de datos.

Si observamos el capítulo quinto del reglamento europeo de protección de datos. Este comienza con el artículo cuarenta y cuatro que nos expresa como primera norma:

> *Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.*

Conociendo esto, tendremos en cuenta el artículo cuarenta y cinco, apartado uno el cual establece:

> *Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.*

en el artículo cuarenta y dos se dictan las condiciones que se deben cumplir para aprobar cláusulas contractuales.

1. *La Agencia Española de Protección de Datos podrá aprobar cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del Reglamento (UE) 2016/679.*

2. *La Agencia Española de Protección de Datos podrá aprobar normas corporativas vinculantes de acuerdo a lo previsto en el artículo 47 del Reglamento (UE) 2016/679. El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de un año. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y se reiniciará tras su notificación a la Agencia Española de Protección de Datos.*

Pero, aunque un país no cuente con la aprobación de la comisión europea, se podrán realizar la transferencia si cumple el artículo cuarenta y tres que dicta:

1. *Supuestos sometidos a autorización previa de la Agencia Española de Protección de Datos. 1.Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679 habrán de ser previamente autorizadas por la Agencia Española de Protección de 47 Datos o, en su caso, autoridades autonómicas de protección de datos, en los siguientes supuestos:*

    a) *cuando la transferencia pretenda fundamentarse en la aportación de cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.*
    b) *Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, en particular a memorandos de entendimiento, siempre que los mismos incluyan derechos efectivos y exigibles para los afectados.*

2. *La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refiere el artículo 64 del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia española de Protección de Datos o, por conducto de la misma, a la Autoridad de control competente, en su caso.*

A continuación, se muestran las referencias al reglamento europeo que se realizan en el artículo cuarenta y tres que referencia al artículo cuarenta y seis apartado dos:

> *Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:*
>
> *a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;*
>
> *b) normas corporativas vinculantes de conformidad con el artículo 47;*
>
> *c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;*
>
> *d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;*
>
> *e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o*
>
> *f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.*

Por último, en el artículo cuarenta y cuatro del anteproyecto de ley se refleja el artículo correspondiente a los Supuestos sometidos a información previa a la autoridad de protección de datos competente

> *Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos. Esta información deberá facilitarse con carácter previo a la realización de la transferencia.*

13. Eliminación de datos personales

En la etapa final del recorrido del flujo de los datos corresponde a la eliminación de estos, al haber terminado el tratamiento de los datos, haber pasado un tiempo superior al permitido para su almacenamiento o la aplicación de los derechos de eliminación por parte de un afectado. La tarea de eliminar los datos corresponde al responsable del tratamiento, lo cual se ve reflejado en el artículo treinta y cuatro, apartado tres del anteproyecto de ley que dicta lo siguiente:

El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos de carácter personal deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

Tenemos que tener en cuenta que la duración de la posesión de los datos dependerá de cómo se haya realizado la toma de los datos siendo

Los datos captados mediante dispositivos de videovigilancia tendrán una duración de un mes, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones y siendo estos puestos en manos de las autoridades y no siendo utilizados para ningún otro propósito.

El anteproyecto de ley y el reglamento de protección de datos europeo no nos da indicaciones claras para la eliminación de los datos, con lo cual son las propias empresas las que deben eliminarlos o subcontratar a empresas especializadas en la eliminación de los ficheros de datos para poder garantizar la eliminación correcta de los datos que está reflejada a lo largo de los reglamentos, la eliminación también deberá realizarse en los datos hechos públicos por el afectado tomando en este caso las medidas que sean posibles.

Como mínimo se deberá hacer un eliminado completo del fichero, es decir no solo eliminar el fichero y mandarlo a la papelera de reciclaje ya que de esta forma no se elimina un fichero, únicamente se mueve a otra carpeta donde van los archivos a eliminar, tendremos que además eliminar de dicha papelera de reciclaje y aun así dicha información podría recuperarse del disco duro, recuérdese que hay que dejar constancia dentro de la empresa de la eliminación del archivo, guardando un registro de quién lo ha eliminado, a qué hora y el motivo de la eliminación.

Como medida a la hora de destruir un disco duro se recomienda tomar registro del disco duro antes de su destrucción, es decir una fotografía con la fecha, hora ,persona que va a destruir el disco duro y la persona que ha mandado su destrucción, después se recomienda destruir el disco duro y romperlo en al menos dos partes con el objetivo de imposibilitar la extracción de información de este, y por último tomar registro de la destrucción, es decir una fotografía del disco duro destruido, la fecha, la hora, la persona que lo ha destruido y la persona que ha mandado su destrucción.

14. Diseño de la página web

Para el desarrollo de la página web donde se ubicarán el test para conocer las carencias de la empresa en relación con el reglamento de protección de datos, se seguirán la metodología para el desarrollo de la web vista en la asignatura impartida en la Universidad politécnica de Valencia “Diseño de Sitios Web”

En primer lugar, la asignatura nos plantea una serie de cuestiones antes de ponerse a realizar el sitio web:

Público objetivo

Toda empresa que desee realizar una auditoría de la empresa con el objetivo de comprobar si están siguiendo correctamente el reglamento de datos de la agencia española de protección de dato, el cual ha entrado en vigor el 25 de mayo de 2018 consiguiendo así adaptarse al reglamento de datos europeo que siguen todos los países de la unión europea.

También puede ser de utilidad para toda persona adulta desconocedora de la ley pero que tenga alguna relación con la empresa como por ejemplo un cliente, el cual quiere comprobar los derechos que este tiene y de si de la empresa está quebrantando la ley.

Por último, el público objetivo también abarca personas que deseen impartir docencia sobre la ley de protección de datos y tener un material de estudio sobre las preguntas de la guía y por qué se realizan.

Que aplicaciones y problemas ayuda a solucionar la web

La aplicación más importante que tiene la web es la de permitir a las empresas realizar auditorías de sus propias empresas para conocer si estos están siguiendo correctamente el nuevo reglamento de protección de datos ya que en caso de no hacerlo podrían tener que enfrentarse a unas sanciones económicas de gran cuantía.

También da una herramienta a empresas dedicadas a realizar auditorías en relación con la protección de datos.

En cuanto a los posibles afectados, da un mecanismo para cuestionar si una empresa está teniendo en cuenta los derechos de los afectados y poder consultar ellos mismos si una empresa está vulnerando los derechos que tienen.

Servir como herramienta de estudio, y permitir a los estudiantes ver qué aspectos se miden a la hora de realizar una auditoría sobre el cumplimiento de los derechos que el reglamento de protección de datos ofrece a sus consumidores.

Herramientas que ofrece la Agencia española de protección de datos

- ### Facilita_RGPD

  Facilita_RGPD es una herramienta fácil y gratuita. Una vez finalizada su ejecución, los datos aportados durante el desarrollo de la misma se eliminan, por lo que la Agencia Española de Protección de Datos en ningún caso puede conocer la información que haya sido aportada.

  Al utilizarla nos comunica si se adapta a los requisitos exigidos para utilizar Facilita_RGPD o si debe realizar un análisis de riesgos.

  no podrá utilizarse para tratamientos que impliquen un alto riesgo para los derechos y libertades de las personas, como datos de salud o tratamientos masivos de datos, entre otros.

  La herramienta genera diversos documentos adaptados a la empresa concreta, cláusulas informativas que debe incluir en sus formularios de recogida de datos personales, cláusulas contractuales para anexar a los contratos de encargado de tratamiento, el registro de actividades de tratamiento, y un anexo con medidas de seguridad orientativas consideradas mínimas.

orientada a empresas que tratan datos personales de escaso riesgo

- ### EVALUA

  Es una herramienta que la AEPD pone a disposición de los responsables de ficheros, de fácil uso, gratuita y que mantiene la anonimidad. Su uso permite a empresas y administraciones autoevaluar el grado de cumplimiento de la Ley Orgánica de Protección de Datos.

  Mediante un auto test basado en preguntas con respuesta múltiple, esta herramienta ofrece respuestas a las dudas a las que se habitualmente se enfrentan quienes manejan datos personales. Su cumplimentación puede ocupar entre 45 y 60 minutos. Una vez finalizado genera un informe con indicaciones y recursos que orientan, en su caso, para cumplir con lo dispuesto en la LOPD.

- ### DISPONE

  La Agencia Española de Protección de Datos facilita a las organizaciones que deben notificar ficheros de titularidad pública la herramienta DISPONE para ayudar a los responsables a elaborar la disposición general o acuerdo de creación, modificación o supresión de los ficheros.

  Incluye ejemplos en cada uno de los aparatados a cumplimentar.

GUIA MODELO DOCUMENTO DE SEGURIDAD

Se ofrece una **GUÍA MODELO** para la elaboración del Documento de Seguridad. Se puede acceder al modelo y descargarlo directamente en su equipo y editarlo en función de sus necesidades.

NOTA

El sistema de Notificaciones Telemáticas de ficheros a la AEPD (NOTA) incluye modelos predefinidos para la notificación de determinados ficheros tipo tanto públicos (Agenda, Control de Accesos, Nóminas, Padrón, Registro…) como privados.

WEBS

- Web del CCN-CERT dirigida fundamentalmente a la Administración Pública donde se encuentran disponibles diversos recursos relacionados con la seguridad de la información tales como la notificación de incidencias de seguridad, herramientas de análisis de riesgos y diversos recursos orientados al cumplimiento del Esquema Nacional de Seguridad.

- Web del Instituto de Ciberseguridad (INCIBE) donde se encuentra disponible diverso material dirigido a la protección de las micropymes y autónomos, tales como herramientas para el autodiagnóstico o formación sobre ciberseguridad.

Información general sobre la organización y la web

Qué

Pregunta	Posible respuesta
Que es el sitio web	Titulo. logos
Que leyes sigue	Texto explicativo
Que ofrece esta página	Texto explicativo

Quién

Pregunta	Posible respuesta
Quien es el alumno y el tutor	Página con texto explicativo

cuando

Pregunta	Posible respuesta
Cuando es válida la ley	Página con texto explicativo

Cómo

Pregunta	Posible respuesta
Como usar la guía	Página con texto explicativo

Donde

Pregunta	Posible respuesta
Donde es de aplicación la guía	Página con texto explicativo

Tipos de contenidos específicos.

Pregunta

Es el contenido principal del sitio web y consiste en una pregunta de un apartado en específico de la guía, dichas preguntas podrán ser respondidas mediante un conjunto de respuestas de selección con las que al final se devolverá un texto con todos los aspectos que la empresa cumple, no cumple o podría mejorar.

Pregunta	Campo	Tipo de campo
Que	Titulo	Texto
	Respuestas	Casillas seleccionables
Quien	Persona con conocimiento de la empresa	Texto
Cuando	Periodos de tiempo	texto
Como	Pregunta formulada de manera que no dé lugar a dudas	texto
Donde	Apartado dentro de la guía	texto

Agrupación de los contenidos

- Guía
  - Será un espacio para poder consultar toda la guía, es decir, la memoria realizada para el trabajo de final de grado
- Formulario
  - Apartado principal de la página web el cual servirá para realizar la auditoria y comprobar que la empresa sigue el anteproyecto de ley aprobado el veinticinco de mayo de dos mil dieciocho.
- Información
  - En este apartado se presentará información de interés sobre la página web, siendo esta: los objetivos, leyes a las que hace referencia, información sobre que no se guarda ningún dato y el alumno y tutor del trabajo de final de grado.
- Herramientas de navegación
  - Tras comprobar que la página no tiene niveles de exploración, se ha llegado a la conclusión que lo más apropiado es la implementación de las herramientas de navegación mediante el uso de una barra de menú simple

Principal	Formulario	Guía	Información

Implementación en Drupal de la barra de menú

La barra de menú se implementará mediante el menú estándar que Drupal ofrece, los cuales generan los bloques de menú que se colocarán en las regiones tal y como se muestra anteriormente.

Implementación en Drupal del formulario

Se implementará mediante el uso del módulo WebForms, se presentará como un conjunto de preguntas y casillas seleccionables, donde habrá preguntas donde serán casillas de selección de si o no como únicas respuestas y otras con un conjunto de respuestas más numerosos.

Módulos instalados en Drupal 7

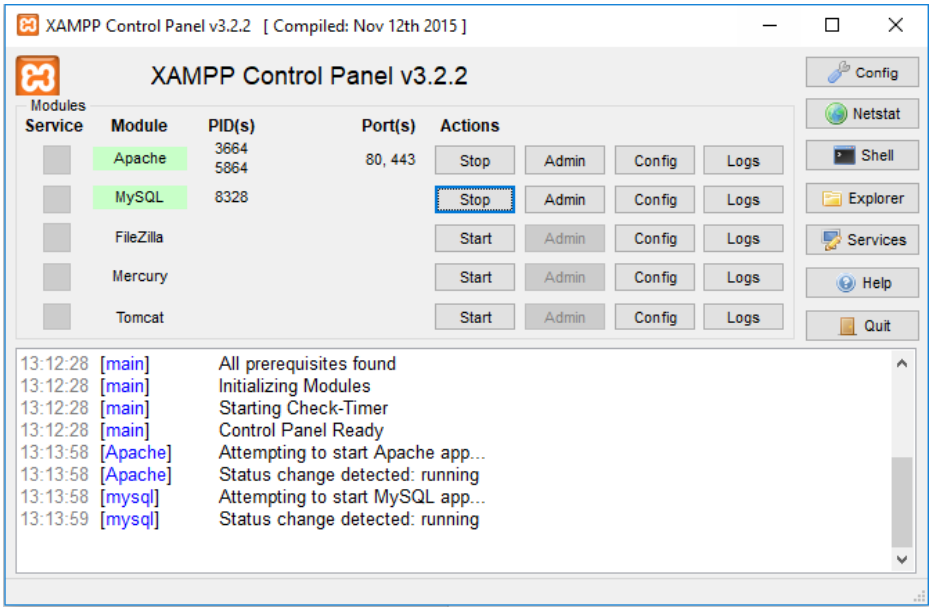
- Webforms 7.x-4.17
- Quiz
- Pdf file
- @font-your-face
- Google fonts
- Ctools 7.x-x.14
- Views 7.x-3.20
- Omega 7.x-3.1(Apariencia)
- Css injector 7.x-1.10
- Omega tools 7.x-3.0-rc4

Instalación de Drupal 7

Para la instalación de Drupal 7 en el equipo se debe instalar primero *Xampp* el cual es un sistema de gestión de bases de datos el cual nos permite crear de manera fácil un servidor local, dicho software es un software libre desarrollado por *Apache*.

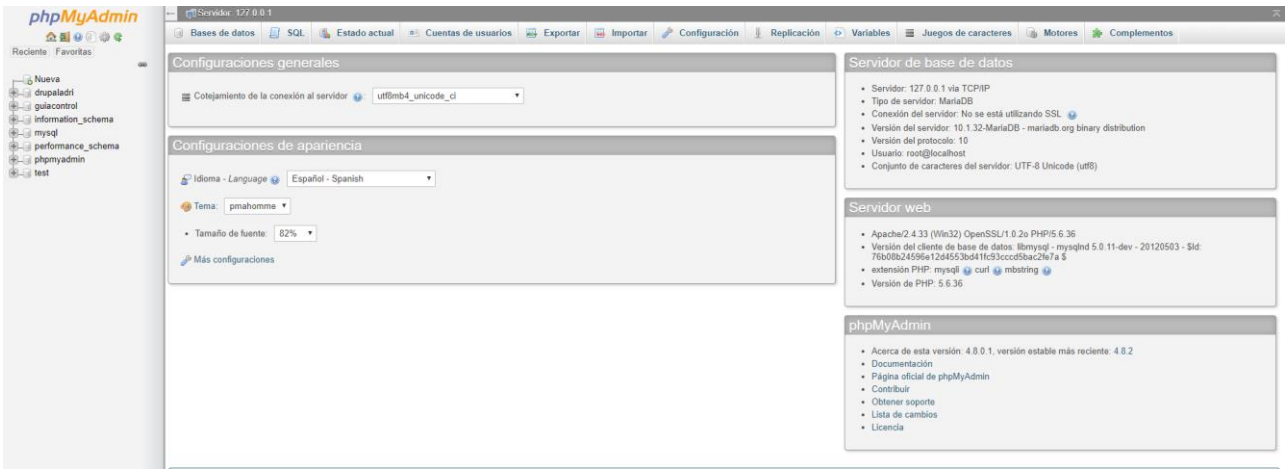
Para su instalación tenemos que acceder a la página web de Apache https://www.apachefriends.org/es/index.html y descargar la versión de instalación 5.6.36.

Una vez instalado bastaría con abrirlo y pulsar *start* en las bases de datos de Apache y MySQL y esperaremos unos cuantos segundos a que dichos módulos aparezcan en color verde tal y como se muestra a continuación.

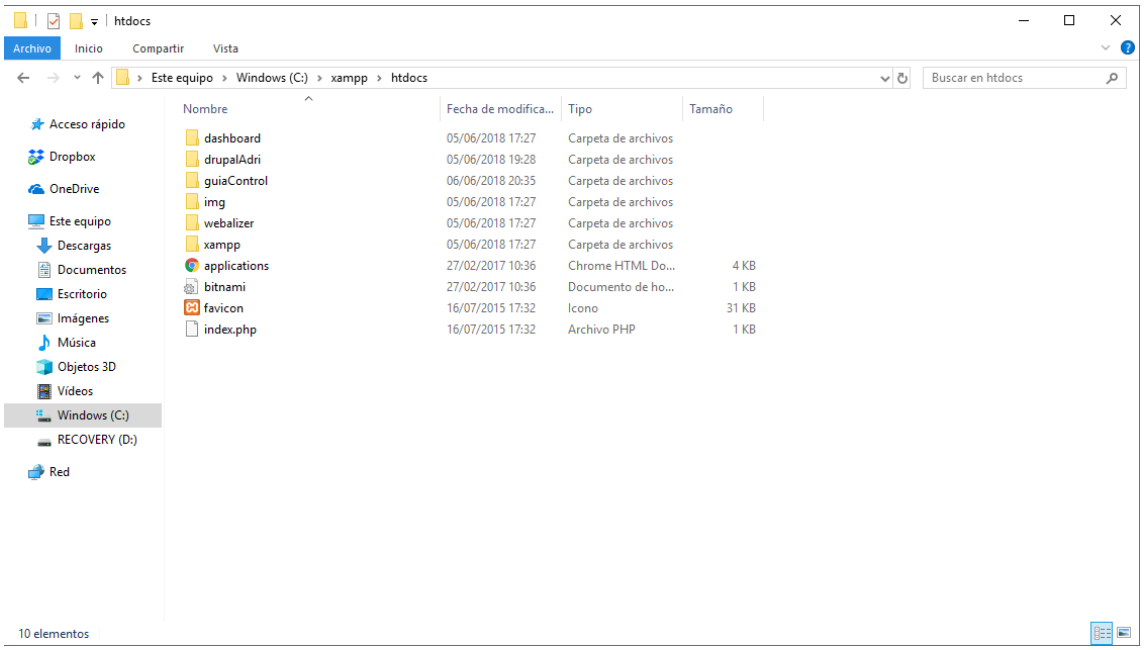


El siguiente paso, consistiría en abrir un explorador de Internet, siendo para el desarrollo de dicho espacio web el explorador *Google Chrome* y a continuación escribir en la barra de búsqueda *localhost*.

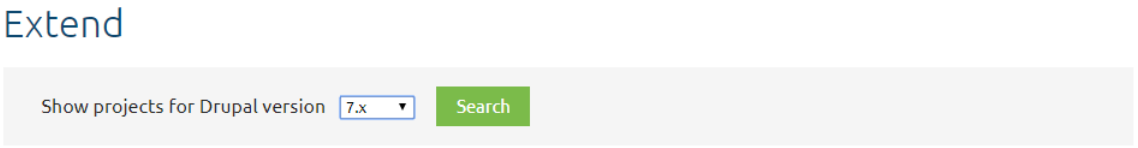
Después si accedemos a *phpMyAdmin* accederíamos al espacio que se muestra a continuación y pulsaríamos sobre nueva para crear una base de datos donde como se puede observar en la imagen está creada la base de datos para el sitio web de la guía de control del cumplimiento de los derechos que el reglamento de protección de datos europeo ofrece a sus consumidores llamada “guiaControl”, además en este lugar podemos exportar e importar bases de datos para migrar la base de datos a otro equipo lo cual tendríamos que realizar si se desease publicar de manera real dicho sitio web.



El siguiente paso consistiría en la instalación del Drupal 7 en el directorio de nuestro equipo: C:\xampp\htdocs y en este lugar depositar la versión de Drupal 7 mostrada a continuación, pero con el nombre de carpeta de nuestro sitio Web.

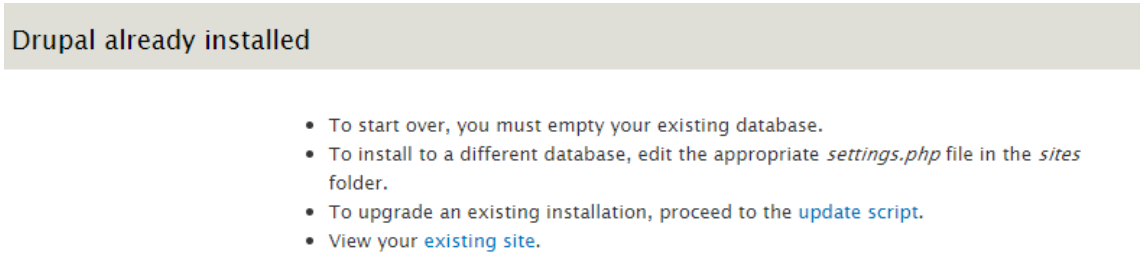


Para la instalación de Drupal 7 accederíamos al sitio web de descarga de Drupal https://www.drupal.org/download y buscaríamos la versión de Drupal 7 siendo está versión muy importante ya que los módulos usados en este trabajo pueden no funcionar en la versión de Drupal 8, al igual que la versión de xampp no funcionaría en Drupal 8.

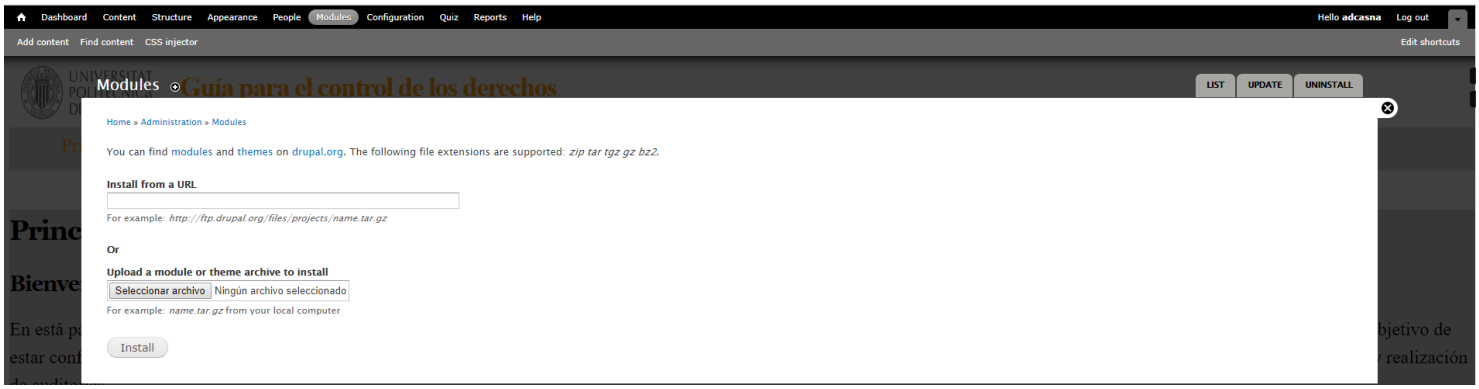


En caso de migración a otro equipo o servidor, deberíamos exportar la carpeta del directorio e importarla en el nuevo equipo o servidor ya que toda la información y características de la página web están en dicha carpeta.

Para el desarrollo de la página web y dicha acción debe realizarse al crear una nueva página web, deberemos acceder a la siguiente dirección http://localhost/guiaControl/install.php y seguir los pasos que nos indica para la instalación de *php*, en caso de que ya esté instalado nos aparecerá el siguiente mensaje.



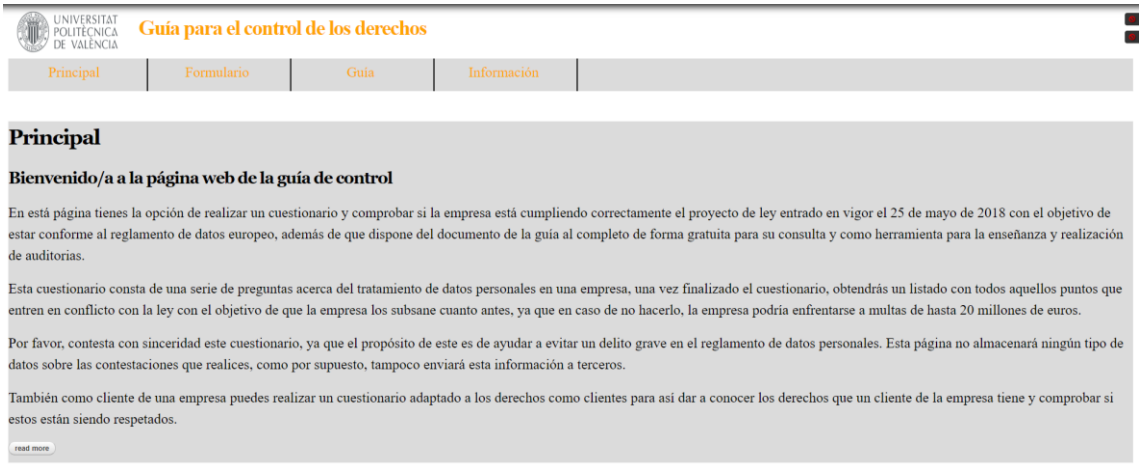
Una vez ya está todo instalado y como último paso para comenzar con el desarrollo de la web tendríamos que instalar los módulos previamente mencionados del siguiente enlace https://www.drupal.org/project/project_module para la versión de Drupal 7 y copiar sus enlaces de descarga en la pestaña de módulos dentro del sitio web y después habilitarlos.



Resultado obtenido

Página principal

Lo primero que encuentran los usuarios en la página principal es un mensaje de bienvenida donde se explican las funcionalidades de la página web, también se solicita a los usuarios que respondan con sinceridad el cuestionario en caso de estar realizando una auditoría real ya que esta página no tiene como objetivo guardar información sobre sus usuarios para después tomar acciones represivas contra ellos.



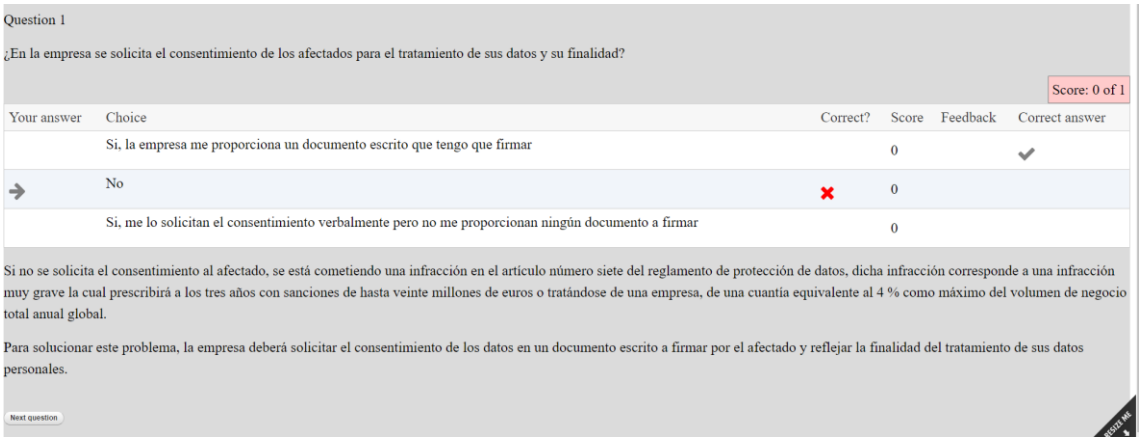
Si accedemos en el menú a la opción de guía, nos mostrara en la propia página web este mismo documento, para que los usuarios tengan la opción de consultarlo en la propia página web y también brindar la opción de descargarlo o imprimirlo.

Si accedemos a la opción de cuestionario en el menú, accederemos a la página que se muestra a continuación. En dicha página se nos presenta dos cuestionarios diferentes: el cuestionario principal de la página de cuarenta y cuatro preguntas siendo este el objetivo de este trabajo final de grado, el cual consiste en el cuestionario para que las empresas realicen auditorías y el cuestionario para clientes, el cual es un formulario en que, como clientes de una empresa, se comprueba si se respetan los derechos fundamentales y comprobables que un cliente puede tener a disposición.

También se ha elegido mostrar información de los test, siendo esta: el número de preguntas, los intentos permitidos, el tiempo que está disponible, el mínimo de puntos para "aprobar este test" y de si se permite ir de nuevo a preguntas anteriores una vez dentro del test.

Se ha elegido que dicha información aparezca en pantalla, para así poder informar a los usuarios de las características del test y de mostrar confianza hacia los usuarios permitiendo realizar el test de la manera que más cómoda le parezca a los usuarios. La característica de la nota de aprobado es para dar una idea de como va la empresa en relación con la ley de protección de datos y de que mediante un número puedan tener una referencia numérica a parte de las soluciones de las preguntas del cuestionario.

Dentro del test podremos contestar las cuestiones planteadas siendo una de estas como ejemplo, la primera pregunta del cuestionario para clientes de una empresa donde de forma premeditada se ha seleccionado una respuesta errónea y como resultado obtenemos la respuesta que se ha seleccionado, junto a la respuesta correcta y la explicación de porqué de esta.


Question 1

¿En la empresa se solicita el consentimiento de los afectados para el tratamiento de sus datos y su finalidad?

Score: 0 of 1

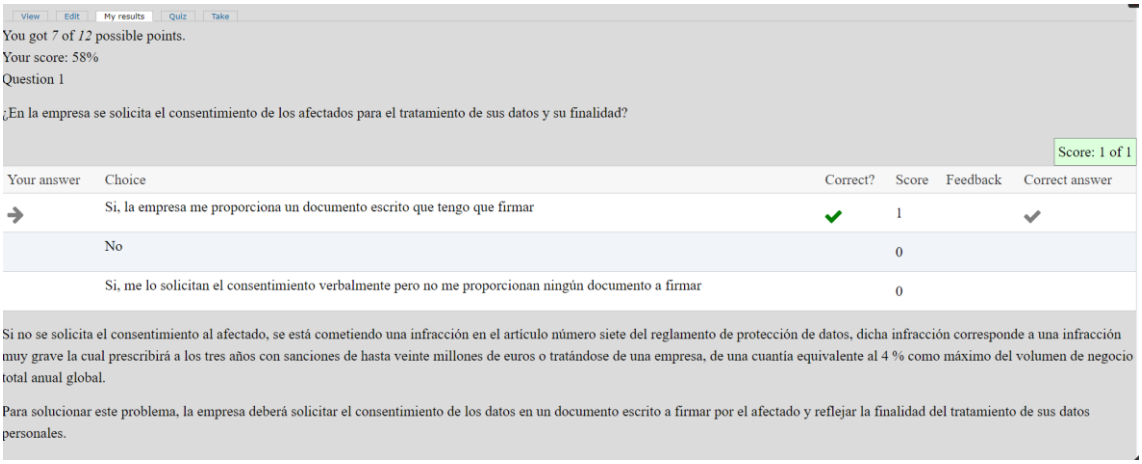
Your answer	Choice	Correct?	Score	Feedback	Correct answer
	Si, la empresa me proporciona un documento escrito que tengo que firmar		0		✔
→	No	✖	0		
	Si, me lo solicitan el consentimiento verbalmente pero no me proporcionan ningún documento a firmar		0		

Si no se solicita el consentimiento al afectado, se está cometiendo una infracción en el artículo número siete del reglamento de protección de datos, dicha infracción corresponde a una infracción muy grave la cual prescribirá a los tres años con sanciones de hasta veinte millones de euros o tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global.

Para solucionar este problema, la empresa deberá solicitar el consentimiento de los datos en un documento escrito a firmar por el afectado y reflejar la finalidad del tratamiento de sus datos personales.

Next question

Una vez finalizado el cuestionario, se nos mostrará una imagen tal y como aparece a continuación en la cual nos mostrará el número de respuesta acertadas, el porcentaje de acierto y luego todas las preguntas juntos a su solución en la misma página.


View | Edit | My results | Quiz | Take

You got *7* of *12* possible points.

Your score: 58%

Question 1

¿En la empresa se solicita el consentimiento de los afectados para el tratamiento de sus datos y su finalidad?

Score: 1 of 1

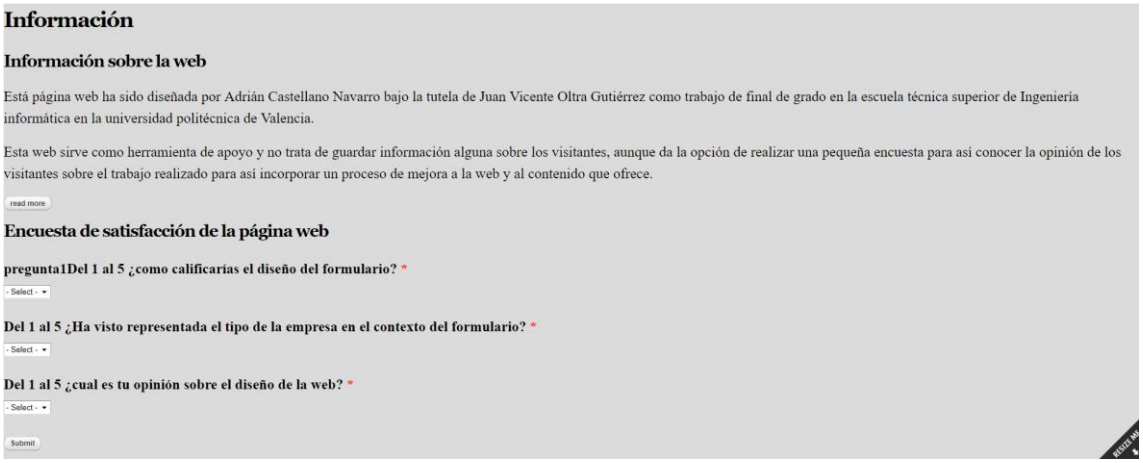
Your answer	Choice	Correct?	Score	Feedback	Correct answer
→	Si, la empresa me proporciona un documento escrito que tengo que firmar	✔	1		✔
	No		0		
	Si, me lo solicitan el consentimiento verbalmente pero no me proporcionan ningún documento a firmar		0		

Si no se solicita el consentimiento al afectado, se está cometiendo una infracción en el artículo número siete del reglamento de protección de datos, dicha infracción corresponde a una infracción muy grave la cual prescribirá a los tres años con sanciones de hasta veinte millones de euros o tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global.

Para solucionar este problema, la empresa deberá solicitar el consentimiento de los datos en un documento escrito a firmar por el afectado y reflejar la finalidad del tratamiento de sus datos personales.

Por último, en la opción de información dentro del menú, donde se muestra información sobre el proyecto de trabajo de final de grado, el tutor, el alumno que ha realizado el trabajo de final de grado, la escuela y la universidad a la que pertenece.

Además, como iniciativa para la mejora continua, se ha desarrollado un pequeño formulario donde se evalúa tanto el espacio web, como los contenidos del mismo.



15. Anexos

Sanciones administrativas

Las sanciones se ven representadas en el artículo setenta que establece quienes son los sujetos responsables:

> *Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y la presente ley orgánica:*
>
> a. *Los responsables de los tratamientos.*
> b. *Los encargados de los tratamientos.*
> c. *Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.*
> d. *Las entidades de certificación.*
> e. *Las entidades acreditadas de supervisión de los códigos de conducta. 63 2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este título.*

Infracciones consideradas muy graves que prescribirán a los tres años con sanciones de hasta veinte millones de euros o tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global (artículo 83.5 del reglamento europeo)

Infracciones muy graves en el apartado de recogida de los datos del cliente

- Que los datos personales no sean recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

- Que el tratamiento no sea licito, es decir que incumpla el artículo seis del reglamento europeo:

    - *El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
    - *El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*

- *el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
- *El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
- *El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
- *El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*
- *Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.*

- Cuando no se sigan las condiciones para recabar el consentimiento del afectado de una manera regular, es decir cuando no siga el artículo siete del reglamento europeo que dicta:
  - *Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.*
  - *Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.*
  - *El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.*
  - *Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.*

Infracciones muy graves en el apartado tratamiento de los datos

- La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.
- El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 10 de esta ley.
- No tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
- No adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
- No exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
- mantenidos de forma que se permita la identificación de los interesados durante más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadístico
- El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 20 de esta ley.
- El tratamiento de datos de carácter personal relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 4.
- La omisión del deber de informar al afectado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 21 de esta ley orgánica. i) La vulneración del deber de confidencialidad establecido en el artículo 6.
- El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.
- El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 29 cuando la misma sea exigible.
- No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.
- La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

Infracciones muy graves en el apartado seguridad de los datos

- El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 20 de esta ley.

Infracciones muy graves en el apartado derechos de los afectados

- La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.
- El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Infracciones muy graves en el apartado transferencias internacionales de datos

- La transferencia internacional de datos de carácter personal a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

Infracciones muy graves en el apartado eliminación de datos personales

- los datos personales no podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado

Infracciones consideradas graves que prescribirán a los dos años con sanciones de hasta diez millones de euros o tratándose de una empresa, de una cuantía equivalente al dos % como máximo del volumen de negocio total anual global (artículo 83.5 del reglamento europeo)

Infracciones consideradas graves en el apartado recogida de los datos del cliente

- El tratamiento de datos de carácter personal de un menor de trece años sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela.

- No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de trece años o por el titular de su patria potestad o tutela sobre el mismo.

Infracciones consideradas graves en el apartado responsable y encargados del tratamiento de los datos

- El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.
- La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.
- La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.
- La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.
- La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento
- No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679. m) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.
- No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.
- El tratamiento de datos de carácter personal sin llevar a cabo una previa valoración de los riesgos que el mismo pudiera generar en los derechos de los afectados, y en particular en su derecho a la protección de datos de carácter personal, conforme a lo dispuesto en el artículo 30.

- El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

Infracciones consideradas graves en el apartado tratamiento de los datos

- La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño y por defecto e integrar las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25.1 del Reglamento (UE) 2016/679.
- La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.
- Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.
- No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.
- No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.
- El tratamiento de datos de carácter personal sin llevar a cabo una previa valoración de los riesgos que el mismo pudiera generar en los derechos de los afectados, y en particular en su derecho a la protección de datos de carácter personal, conforme a lo dispuesto en el artículo 30.
- El tratamiento de datos de carácter personal sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

Infracciones consideradas graves en el apartado seguridad de los datos

- El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento
- El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.
- El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

Infracciones consideradas graves en el apartado códigos de conducta/tipo

- El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente. Dicho artículo cuarenta y uno dicta:
    - Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.
    - 2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:
        a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;
        b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;
        c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y
        d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.
    - 3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los criterios de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.
    - 4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.
    - 5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.
    - 6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

- La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso de que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Infracciones consideradas graves en el apartado derechos de los afectados

- El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

Infracciones consideradas leves las cuales son de carácter meramente formal y prescribirán al año. De igual forma que las sanciones graves, estás impondrán multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

Infracciones consideradas leves en el apartado responsable y encargados del tratamiento de los datos

- No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.
- La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.
- El incumplimiento por encargado o subencargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la 70 legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.
- Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarla una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

Infracciones consideradas leves en el apartado tratamiento de los datos

- La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.
- Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.
- La notificación incompleta o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.
- Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarla una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.
- No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 35.3 de esta ley orgánica.

Infracciones consideradas leves en el apartado seguridad de los datos

- La notificación incompleta o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.
- El incumplimiento de la obligación de documentación de cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.
- El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73.q) de esta ley orgánica.

Infracciones consideradas leves en el apartado códigos de conducta/tipo

- El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Infracciones consideradas leves en el apartado derechos de los afectados

- El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.
- La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.
- No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.
- No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73.c).
- El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.
- El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.
- El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3.
- No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73.q) de esta ley orgánica.

Preguntas del cuestionario

A continuación, se incluyen las preguntas que se han elegido a la hora de realizar los cuestionarios, tanto el cuestionario dirigido a las empresas, como al cuestionario dirigido a los clientes

Cuestionario del reglamento de protección de datos para empresas

- ¿En la empresa se solicita el consentimiento de los afectados para el tratamiento de sus datos y su finalidad?
- ¿En la empresa se realiza el tratamiento de los datos personales del afectado para otras finalidades de las que están acordadas con el cliente?
- Si en la empresa trata datos de personas menores de edad ¿solicita el consentimiento en un documento con un lenguaje sencillo o explicado verbalmente al tratarse de una persona mayor de trece años?
- ¿Si en la empresa trata los datos de una persona fallecida, se pone en contacto con sus familiares para explicarle sus derechos en relación a los datos personales?
- ¿En la empresa trata datos como la orientación sexual, afiliación política, origen étnico, creencias religiosas sin ser estos necesarios para el interés público general y/o interés público en el ámbito de la salud?
- Si la empresa hace uso de videovigilancia. ¿señaliza de su uso con un cartel informativo indicando su presencia?
- Si la empresa hace uso de videovigilancia. ¿Las cámaras están dirigidas a la vía pública?
- ¿La empresa asigna a un encargado al tratamiento de los datos?
- ¿Asigna la empresa un delegado de protección de datos en el caso de que el tratamiento de los datos sea llevado a cabo por un organismo público exceptuando el caso de los tribunales que actúen en ejercicio de su función judicial?
- ¿Asigna la empresa un delegado de protección de datos en el caso de que el tratamiento de los datos suponga una observación habitual y sistemática de interesados a gran escala?
- En el caso en que la empresa sea un colegio profesional y/o un consejo general sobre colegios profesionales ¿Asigna la empresa un delegado de protección de datos?

- En el caso en que la empresa sea un centro docente, una universidad pública o una universidad privada ¿Asigna la empresa un delegado de protección de datos?

- En el caso en que la empresa sea una entidad que exploten redes y presten servicios de comunicaciones ¿Asigna la empresa un delegado de protección de datos?

- En el caso en que la empresa sea un establecimiento financiero de crédito ¿Asigna la empresa un delegado de protección de datos?

- En el caso en que la empresa sea una entidad aseguradoras o reaseguradoras ¿Asigna la empresa un delegado de protección de datos?

- En el caso en que la empresa sea una empresa de servicios de inversión ¿Asigna la empresa un delegado de protección de datos?

- En el caso en que la empresa asigne a un delegado de protección de datos ¿está este debidamente cualificado?

- ¿La empresa obliga al delegado a actuar en conveniencia de los propósitos de la empresa?

- Si la empresa desea utilizar los datos personales de un cliente para otra finalidad de la acordada con este ¿La empresa se pone en contacto con el cliente para solicitar su consentimiento?

- ¿La empresa toma medidas para mantener actualizados los datos de los afectados? siendo 5 para medidas muy estrictas y 1 si no se actualizan los datos de los clientes

- ¿En la empresa se guarda secreto de confidencialidad con los datos de los afectados?

- ¿Encarga los datos a un tercero sin ningún tipo de contrato?

- ¿La empresa solicita a los afectados más datos de los necesarios para el desarrollo de la función?

- ¿La empresa facilita el acceso al personal de la Agencia española de protección de datos?

- ¿Son mantenidos los datos de forma que se permita la identificación de los interesados durante más tiempo del necesario para los fines del tratamiento de los datos personales?

- ¿La empresa diferencia entre documentos con un nivel de seguridad de nivel bajo, medio y alto? siendo 5 los tres tipos de documentos y 1 si no se diferencian

- ¿La empresa tiene un sistema de identificación y autentificación con un nivel de seguridad aceptable dependiendo del tipo de datos?

- ¿La empresa asigna un responsable de seguridad al documento?

- ¿La empresa tiene procedimientos para tratar los casos de copias, traslados, resolución de incidencias y eliminación de datos? Siendo 5 si la empresa tiene dichos procedimientos y 1 si no tiene ningún procedimiento para estos casos

- ¿La empresa realiza auditorias como mínimo cada dos años si esta trata con documentos con un nivel de seguridad requerido alto?

- ¿Si la empresa utiliza un código de conducta, está este dado de alta en la agencia española de protección de datos?

- ¿Si la empresa ha cometido alguna infracción y se ve obligado a utilizar un código de conducta, está siendo utilizado dicho código dentro de la empresa?

- ¿Ofrece la empresa derecho de acceso a los afectados?

- ¿Ofrece la empresa derecho de rectificación a los afectados?

- ¿Ofrece la empresa derecho de supresión a los afectados?

- ¿Ofrece la empresa derecho de limitación del tratamiento a los afectados?

- ¿Ofrece la empresa derecho de portabilidad a los afectados?

- ¿Ofrece la empresa derecho de oposición a los afectados?

- ¿La empresa cobra un canon para que los afectados puedan acceder a sus derechos?

- ¿La empresa transfiere datos personales a países fuera de la unión europea que no tiene un documento donde se refleje que tenga garantías para poder realizar transferencias de datos?

- ¿La empresa realiza una destrucción completa del fichero de datos personales? 5 si se utilizan técnicas de destrucción de ficheros (como una eliminación completa o la contratación de una empresa especializada en esta tarea) y 1 si no se destruyen

- ¿La empresa cambia con cierta regularidad los discos duros de los equipos que realicen el tratamiento de datos? si se cambian regularmente y 1 si no se cambian nunca.

- ¿La empresa destruye físicamente los discos duros cuando estos han perdido su utilidad o se han estado utilizando durante mucho tiempo?

- ¿Si la empresa contrata una empresa tercera especializada en la destrucción de material, está dicha empresa debidamente cualificada?

Cuestionario del reglamento de protección de datos para clientes

- ¿En la empresa se solicita el consentimiento de los afectados para el tratamiento de sus datos y su finalidad?

- Si en la empresa trata datos de personas menores de edad ¿solicita el consentimiento en un documento con un lenguaje sencillo o explicado verbalmente al tratarse de una persona mayor de trece años?

- ¿Si en la empresa trata los datos de una persona fallecida, se pone en contacto con sus familiares para explicarle sus derechos en relación a los datos personales?

- Si la empresa hace uso de videovigilancia. ¿señaliza de su uso con un cartel informativo indicando su presencia?

- Si la empresa hace uso de videovigilancia. ¿Las cámaras están dirigidas a la vía pública?

- ¿La empresa solicita a los afectados más datos de los necesarios para la finalidad perseguida por la empresa?

- ¿Ofrece la empresa derecho de acceso a los afectados?

- ¿Ofrece la empresa derecho de rectificación a los afectados?

- ¿Ofrece la empresa derecho de supresión a los afectados?

- ¿Ofrece la empresa derecho de limitación del tratamiento a los afectados?

- ¿Ofrece la empresa derecho de portabilidad a los afectados?

- ¿La empresa cobra un canon para que los afectados puedan acceder a sus derechos?

16. Conclusión

A lo largo de este trabajo se ha desarrollado una guía con la que se puede comprobar si una empresa está cumpliendo correctamente el reglamento de protección de datos y en base a esta guía se ha desarrollado una página web en la cual tanto una empresa como un cliente pueden evaluar mediante un cuestionario si dicha empresa cumple correctamente el reglamento de protección de datos.

Gracias a las indicaciones y a la documentación otorgada por el tutor de este proyecto pude comenzar un trabajo de investigación donde leía y resumía toda la documentación que el me proporcionaba, comenzando por el anteproyecto de ley, pasando después al reglamento de protección de datos europeo 2016/679 donde comprobaba las referencias del anteproyecto de ley con este documento. También realicé un documento donde analizaba la documentación de la agencia española de protección de datos y el reglamento e-privacy.

El principal problema con el que me encontré fue el modo de estructurar el trabajo ya que los reglamentos tienen una gran cantidad de artículos y realizar la guía con una estructuración correcta era un objetivo indispensable.

Otro de los problemas que me he encontrado en este proyecto ha sido el cambio de la página web de la agencia española de protección de datos, ya que, con la entrada en vigor de la nueva ley, cambiaron su página web y toda la documentación fue eliminada para los usuarios por lo que ya no se pueden consultar las herramientas a las que se hacen referencia en el desarrollo de este trabajo.

También he encontrado otro problema a la hora de realizar el cuestionario y ha sido la envergadura de dicho cuestionario ya que, al ser un reglamento con tantos puntos a tener en cuenta, se ha vuelto una tarea complicada mantener la relación entre la velocidad con la que un usuario pueda realizar una auditoría completa utilizando la herramienta y que dicho cuestionario abarque todos los puntos donde poder evaluar a una empresa en relación al reglamento de protección de datos.

En cuanto a mi valoración de este proyecto puedo decir que estoy satisfecho con el trabajo realizado en este proyecto, ya que he podido realizar una tarea de investigación que me ha permitido aprender sobre la nueva legislación además de poder utilizar los conocimientos adquiridos en el grado de ingeniería informática para el desarrollo de la página web, además de haber podido realizar una herramienta mediante Drupal 7 que puede ser de utilidad para un gran número de personas.

17. Bibliografía

Reglamentos.

- Anteproyecto de ley orgánica de protección de datos de carácter personal. 29 de junio 2018. http://servicios.mpr.es/seacyp/search_def_asp.aspx?crypt=xh%8A%8Aw%98%85d%A2%B0%8DNs%90%8C%8An%87%A2%7F%8B%99tt%84sm%A3%91
- Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016.20 junio 2018. https://www.boe.es/doue/2016/119/L00001-00088.pdf
- Reglamento e-privacy.7 de abril 2018. https://iabspain.es/wp-content/uploads/faq-reglamento-e-privacy.pdf

Documentación.

- Documentación empresa de tipo privada. 2 de julio 2018. https://es.wikipedia.org/wiki/Empresa_privada
- Documentación empresa de tipo pública. 2 de julio 2018. https://es.wikipedia.org/wiki/Empresa_p%C3%BAblica
- Definición del tratamiento de datos personales.16 de mayo 2018 http://www.cuidatusdatos.com/infotratamiento.html

Trabajo de final de grado del alumno Álvaro Morro Ibáñez.

- Creación de una aplicación de apoyo a los cambios normativos en protección de datos. 6 de julio 2018. https://riunet.upv.es/bitstream/handle/10251/88478/MORRO%20-%20Creaci%C3%B3n%20de%20una%20aplicaci%C3%B3n%20de%20apoyo%20a%20los%20cambios%20normativos%20en%20protecci%C3%B3n%20de%20datos.pdf?sequence=1&isAllowed=y

Herramientas de la Agencia Española de protección de datos.

- Colección de códigos de conducta (En construcción) 23 de mayo 2018. https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php
- Ejemplo de código de conducta de empresa seguro de automóvil (En construcción) 20 de mayo 2018 https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/pdfs/CODIGO_TIPO_DE_FICHERO_HISTORICO_DE_SEGUROS_DEL_AUTOMOVIL-UNESPA-2017.pdf

- Información de registro de un código de conducta (En construcción) 24 de mayo 2018. https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/resoluciones/CT-0002-2000_Resolucion_16_11_2009.pdf